



New Features Guide

FortiManager 7.4.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



June 20, 2023

FortiManager 7.4.0 New Features Guide

02-740-898074-20230831

TABLE OF CONTENTS

Change Log	6
Overview	7
Device Manager	8
Device and Groups	8
Auto-link setting is exposed to control configuration installation during ZTP 7.4.1	8
SD-WAN	11
Automated SD-WAN post overlay process creates policies to allow the health-checks traffic to flow between Branch and HUB	12
Automated SD-WAN overlay process adds "branch_id" meta variable auto assignment	15
SD-WAN monitoring map integrates with Cloud Assisted Monitoring Service to allow FortiGate interface speed tests from inside FortiManager	16
SDWAN monitoring map enhancements	19
SDWAN template for heterogeneous WAN link types	23
Templates	25
Preview CLI configuration for the device provisioning templates	25
Fortinet factory-default wireless and extender templates	28
Jinja Templates have direct access to the device DB to support generation of dynamic configuration	34
Fabric Authorization Template is integrated with Device Blueprint and supports meta variables 7.4.1	41
Central Management	46
AP Manager	46
Multiple optimizations to the factory default SSID and AP-profiles 7.4.1	46
FortiSwitch Manager	50
Per-device VRRP mapping can be used under FortiSwitch Profiles	50
FortiManager allows switchport export to another VDOM, and configuration of the exported port in the destination VDOM	51
FortiSwitch replacement procedure can be executed from FortiManager GUI	54
Custom commands can be assigned/unassigned at once to multiple managed FortiSwitches 7.4.1	56
Others	59
FortiManager supports install preview for model devices	59
VPN Monitoring displays IPsec VPN tunnels created by IPsec templates and SD-WAN overlay wizard	64
FortiManager supports CLI diff in the workflow approval sessions	67
Internet Service database update occurs only if specific policy objects require a FortiGuard update 7.4.1	69
Policy and Objects	71
Policy	71
Install preview support for partial install	71
Policy Package installation added link to the progress report page for installation errors	78
Support for IoT Virtual Patching in NAC policies using pre-built severity filters	82

Policy deletion warning message improved with selected policy number and name reference 7.4.1	83
Enable option for persistent policy hit-count on ADOM database 7.4.1	84
Partial install pushes only the instructed configuration (JSON API) 7.4.1	85
Policy partial install supports policy reorder/move operation (JSON API) 7.4.1	87
System	92
High Availability (HA)	92
FortiManager supports different VM type platforms to form the FortiManager cluster ...	92
ADOM	93
ADOM 7.2 Policy Package supports installation on FortiGate 7.4 7.4.1	93
7.2 ADOM managing mixed FOS versions 7.4.1	96
FortiManager can upgrade multiple ADOMs (same version) at the same time 7.4.1	98
Others	99
Block out contract device from upgrading to next or major or minor release	100
Automatic system backup setup in GUI to configure a backup schedule and visualize backup history 7.4.1	102
Cloud Services	105
FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS	105
Other	111
New FortiManager UX design	111
Dashboard	111
Policy & Objects	113
AP Manager	114
Management Extensions	115
System Settings	116
Fabric and External connector pages have been reorganized for an enhanced user experience	121
FortiManager connector relay to AWS will proxy all individual FortiGate requests	125
FortiManager key areas have been reorganized to enhance user experience	126
Device Manager	126
Firewall Objects	134
Fabric Connector	135
Firewall Policies	136
FortiAP Manager	136
FortiSwitch Manager	139
FortiManager imports EPGs entries using the Cisco ACI connector as individual objects	140
Index	144
7.4.0	144
Device Manager	144
Central Management	144
Policy and Objects	145
System	145
Cloud Services	145
Other	145
7.4.1	145
Device Manager	145

Central Management	146
Policy and Objects	146
System	146

Change Log

Date	Change Description
2023-05-15	Initial release.
2023-06-20	Added: <ul style="list-style-type: none">• FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS on page 105• FortiManager imports EPGs entries using the Cisco ACI connector as individual objects on page 140• FortiSwitch replacement procedure can be executed from FortiManager GUI on page 54• Support for IoT Virtual Patching in NAC policies using pre-built severity filters on page 82
2023-08-31	Initial release of FortiManager 7.4.1.

Overview

This guide provides details of new features introduced in FortiManager 7.4. For each feature, the guide provides detailed information on configuration, requirements, and limitations, as applicable.

The FortiManager new features are organized into the following categories:

- [Device Manager on page 8](#)
- [Central Management on page 46](#)
- [Policy and Objects on page 71](#)
- [System on page 92](#)
- [Cloud Services on page 105](#)
- [Other on page 111](#)

For a list of all features organized by the version number that they were introduced, see [Index on page 144](#).

Device Manager

This section lists the new features added to FortiManager for the device manager:

- [Device and Groups on page 8](#)
- [SD-WAN on page 11](#)
- [Templates on page 25](#)

Device and Groups

This section lists the new features added to FortiManager for devices and groups:

- [Auto-link setting is exposed to control configuration installation during ZTP 7.4.1 on page 8](#)

Auto-link setting is exposed to control configuration installation during ZTP - 7.4.1



This information is also available in the FortiManager 7.4 Administration Guide:

- [Adding offline model devices](#)
- [Adding a model FortiGate HA cluster](#)

The auto-link setting is exposed in the model device wizard to allow administrators to better control configuration installation during the ZTP process.

To configure the auto-link setting for ZTP:

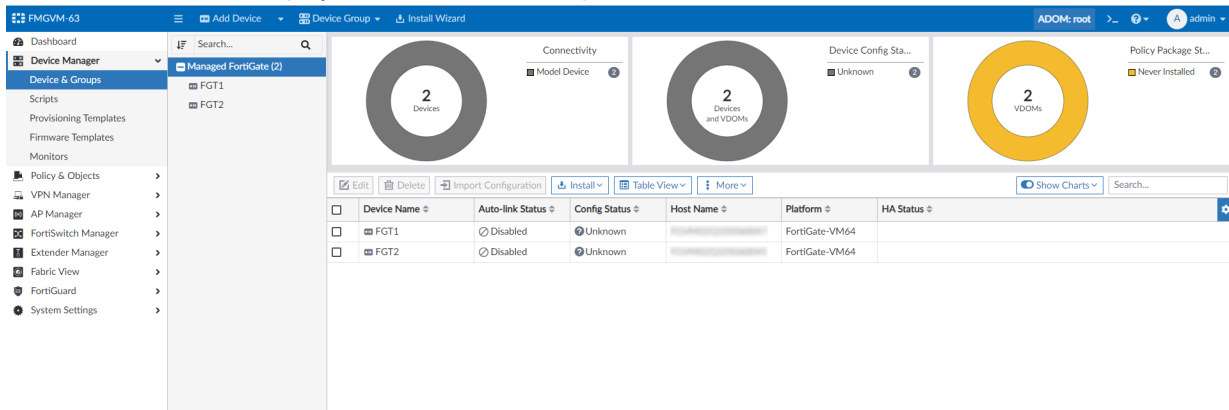
1. In the *Add Model Device* wizard, the option to *Automatically Link to Real Device* can be disabled or enabled.

The screenshot shows the FortiManager 7.4.0 interface with the 'Add Device - Provide Model Device Info (1/2)' wizard open. The wizard is titled 'Add Model Device' and contains the following fields and options:

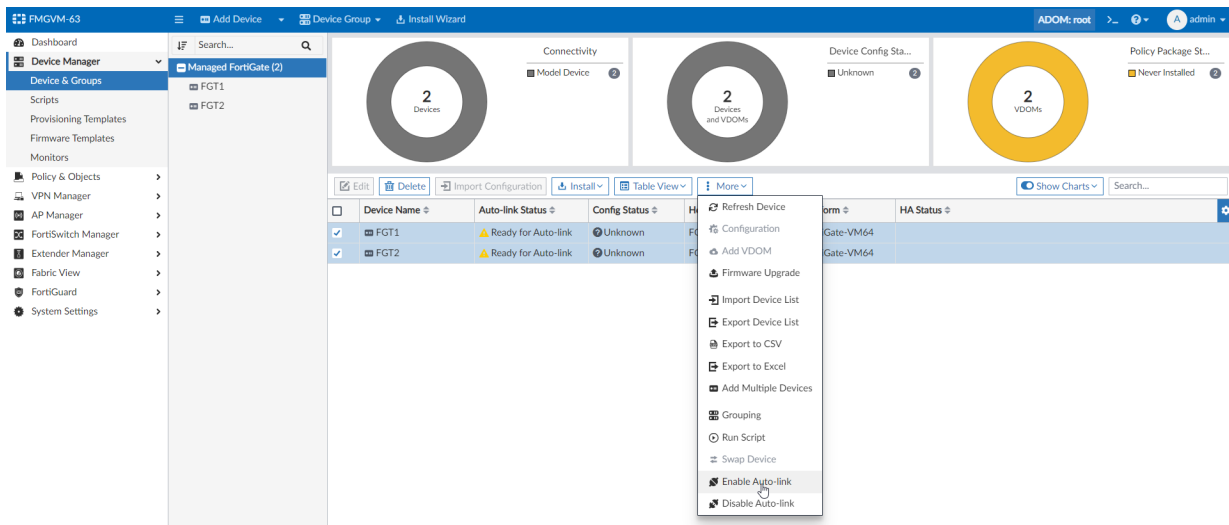
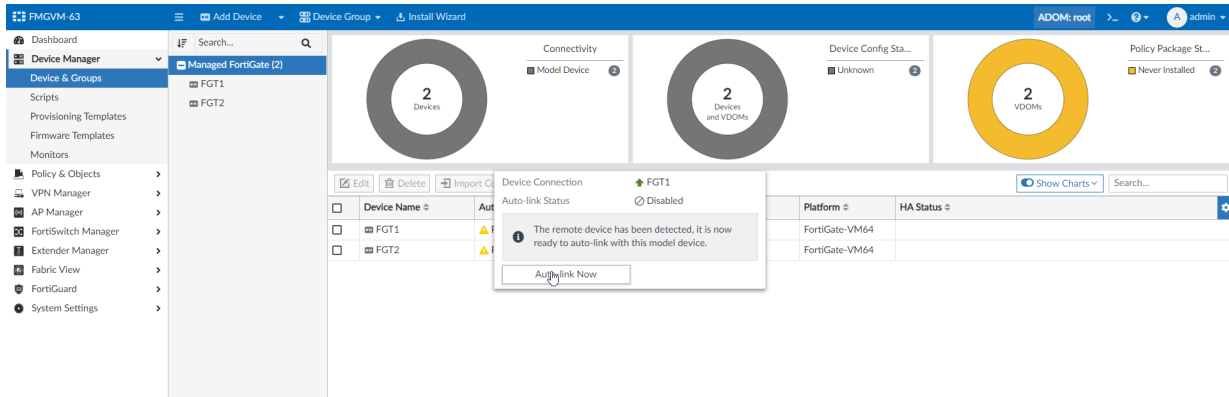
- Name: FGT1
- Link Device By: Serial Number (selected), Pre-shared Key
- Serial Number: [Empty field]
- Use Device Blueprint: [Off]
- Device Model: FortiGate-VM64 (selected)
- Port Provisioning: 1 (selected)
- Automatically Link to Real Device: [On]
- Enforce Firmware: 7.4 (By Default) (selected)
- Add to Device Group: [Off]
- Add to Folder: [Off]
- Fabric Authorization Template: [Off]
- Pre-Run CLI Template: [Off]
- Assign Policy Package: [Off]
- Provisioning Templates: [Off]
- Metadata Variables: [Off]
- Copy Device Dashboard: Click to select

At the bottom of the wizard, there are three buttons: '< Back', 'Next >', and 'Cancel'.

2. The auto-link status is displayed in the *Device Manager*.



3. Auto-link can be enabled from the tool tip for single device, or by choosing multiple devices and selecting the *Enable Auto-link* setting in the *More* dropdown menu.



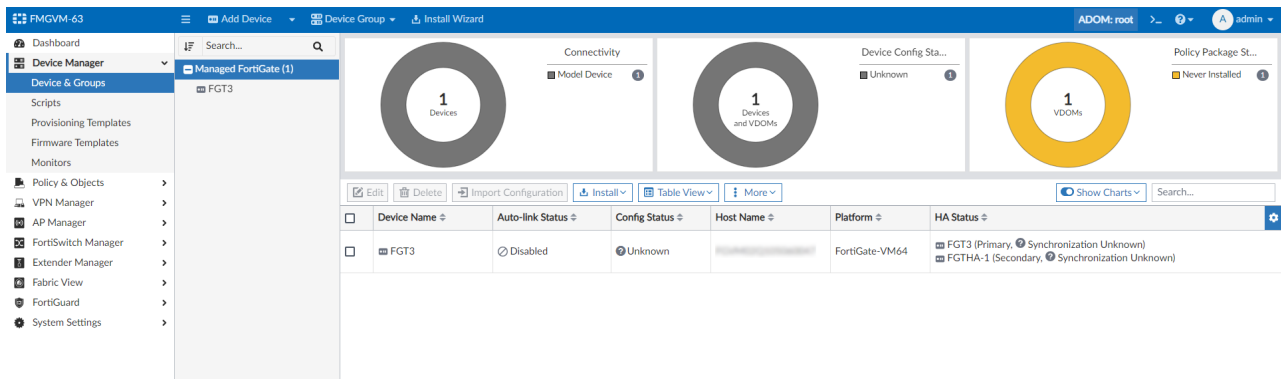
4. If for any reason auto-linking fails, you can try it again after the issue is resolved by clicking *Retry Auto-link*.

The top screenshot shows the FortiManager Device Manager interface. The left sidebar contains the navigation menu. The main area displays three donut charts: Connectivity (1 Device), Device Config Sta... (1 Device and VDOMs), and Policy Package St... (1 Never Installed). Below the charts is a table with columns: Device Name, Auto-link Status, Config Status, Host Name, Platform, and HA Status. The table contains one entry: FGT1, with Auto-link Status 'Last Try Failed', Config Status 'Unknown', Host Name 'FGTVM64-94', Platform 'FortiGate-VM64', and HA Status empty.

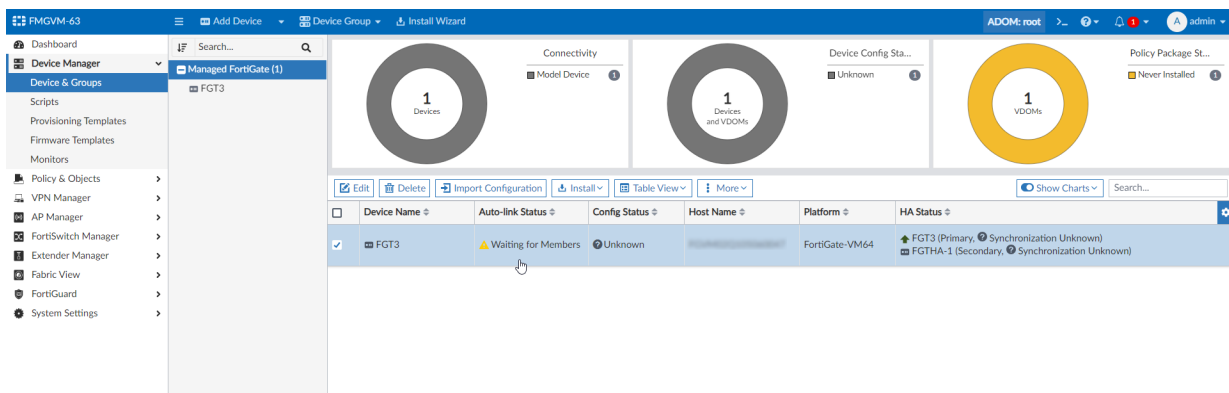
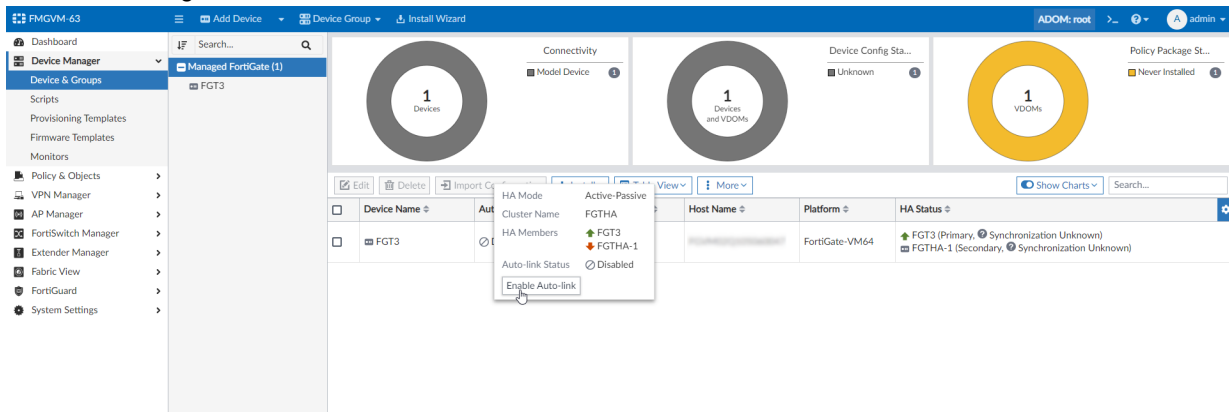
The bottom screenshot shows the same interface, but the Auto-link Status for FGT1 is now 'Enabled'. A context menu is open over the 'Auto-link Status' column, showing options: 'Disable Auto-link' and 'Retry Auto-link'.

5. In the Add Model HA Cluster wizard, the option to *Automatically Link to Real Device* can be disabled or enabled.

The screenshot shows the 'Add Device - Provide Model HA Cluster Info (1/2)' wizard. The 'Add Model HA Cluster' section includes fields for Name (FGT3), HA Mode (Active - Passive), Cluster ID (100), Cluster Name (FGTHA), Password, Link Device By (Serial Number), Serial Number (0047), Device Model (FortiGate-VM64), and Priority (200). The 'HA Secondary' section includes fields for Serial Number (0045), Priority (100), and Action. The 'Add to Device Group' section includes checkboxes for 'Automatically Link to Real Device' (checked), 'Enforce Firmware' (7.4.0-b2360), 'Fabric Authorization Template', 'Pre-Run CLI Template', 'Assign Policy Package', and 'Provisioning Templates'. The bottom of the wizard has '< Back', 'Next >', and 'Cancel' buttons.



6. After auto-linking is enabled, auto-link will be started after all cluster members are connected.



SD-WAN

This section lists the new features added to FortiManager for SD-WAN:

- Automated SD-WAN post overlay process creates policies to allow the health-checks traffic to flow between Branch and HUB on page 12
- Automated SD-WAN overlay process adds "branch_id" meta variable auto assignment on page 15
- SD-WAN monitoring map integrates with Cloud Assisted Monitoring Service to allow FortiGate interface speed tests from inside FortiManager on page 16

- SDWAN monitoring map enhancements on page 19
- SDWAN template for heterogeneous WAN link types on page 23

Automated SD-WAN post overlay process creates policies to allow the health-checks traffic to flow between Branch and HUB



This information is also available in the FortiManager 7.4 Administration Guide:

- [Configuring an SD-WAN overlay template](#)

Automated SD-WAN post overlay process creates policies to allow the health-checks traffic to flow between Branch and HUB.

The SD-WAN overlay template includes two new options in the wizard to automate the post-wizard processes. The SD-WAN overlay template example configured in this document uses a dual-hub topology.

1. Normalize Interfaces

Enable the *Normalize Interfaces* option to normalize the SD-WAN zones created by the template.

- The following normalized interface is created for the SD-WAN Hub(s):
 - *HUB-Lo* with *Per-Device Mapping* to *HUB1-Lo* for the HUB 1 device and *HUB2-Lo* from the HUB 2 device.

Mapped Device	Details	Type	Addressing Mode	IP/Netmask	Shaping Profile
FGT_HUB1(root)	HUB1-Lo				
FGT_HUB2(root)	HUB2-Lo				

- The following normalized interfaces are created for branch devices:
 - The *HUB1 SD-WAN zone* is mapped per-platform to *HUB1*.

Edit Normalized Interface

Name: HUB1
Description: Created by SDWAN Overlay Template
Color: Change
Wildcard:

Per-Platform Mapping

Name	Device Interface Name	Shaping Profile
all	HUB1	

Per-Device Mapping

Revision

Change Note*

OK Cancel

- The *HUB2 SD-WAN zone* is mapped per-platform to *HUB2*.

Edit Normalized Interface

Name: HUB2
Description: Created by SDWAN Overlay Template
Color: Change
Wildcard:

Per-Platform Mapping

Name	Device Interface Name	Shaping Profile
all	HUB2	

Per-Device Mapping

Revision

Change Note*

OK Cancel

- VPN IPsec tunnel templates are created for HUB interfaces when using the SD-WAN overlay template. When *Normalized Interface* is enabled, normalized interfaces for the VPNs are added to the normalized interface list.

2. Add Health Check Firewall Policy to Hub/Branch Policy Package

Enable the *Add Health Check Firewall Policy to Hub/Branch Policy Package* option to create health check firewall policies (or policy blocks) for HUB(s) and branches.

- Users must select the HUB and branch policy package that will be used during the wizard configuration. You can select an existing policy package or create a new one.

Edit SD-WAN Overlay Template - SD-WAN Template Options (4/5)

Add Overlay Objects to SD-WAN Template	<input checked="" type="radio"/>	sd-wan	<input type="button" value="x"/> ▼
Add Overlay Interfaces and Zones	<input checked="" type="radio"/>		
Add Health Check Servers for Each HUB as Performance SLA	<input checked="" type="radio"/>		
Normalize Interfaces	<input checked="" type="radio"/>		
Add Health Check Firewall Policy to Hub Policy Package	<input checked="" type="radio"/>	Hub-p1	<input type="button" value="x"/> ▼
Add Health Check Firewall Policy to Branch Policy Package	<input checked="" type="radio"/>	Branch-p1	<input type="button" value="x"/> ▼

- Based on the selection, firewall policies (or policy blocks) are created to allow SLA health checks to each device loopback.
- The SD-WAN overlay template creates the policy block and applies it to the top of the HUB Policy Package.

Search...		+ Create New	Edit	Delete	Section	Policy Block	Policy Lookup	Collapse All	Search...
Branch-p1	Firewall Policy	Installation Targets	CLI Configurations	Hub-p1	Firewall Policy	Installation Targets	CLI Configurations	default	Policy Blocks (1)
#	Name	From	To	Source	Destination	Schedule			
sd-wan-overlay_HBLK (1/1 Total:1)									
1	Health Check Access	VPN1	HUB-Lo	sd-wan-overlay_O	sd-wan-overlay_Lc	always			
Implicit (2/2 Total:1)									
2	Implicit Deny	any	any	all	all	always			

- A policy block is not created for the SD-WAN branch Policy Package.

Search...		+ Create New	Edit	Delete	Section	Policy Block	Policy Lookup	Collapse All	Search...
Branch-p1	Firewall Policy	Installation Targets	CLI Configurations	Hub-p1	Firewall Policy	Installation Targets	CLI Configurations	default	Policy Blocks (1)
#	Name	From	To	Source	Destination	Schedule			
Implicit (1/1 Total:1)									
1	Implicit Deny	any	any	all	all	always			

Automated SD-WAN overlay process adds "branch_id" meta variable auto assignment



This information is also available in the FortiManager 7.4 Administration Guide:

- [Configuring an SD-WAN overlay template](#)
- [Objects and templates created by the SD-WAN overlay template](#)

The automated SD-WAN overlay process adds "branch_id" meta variable auto assignment.

To automatically assign branch IDs using the SD-WAN overlay template:

1. Go to *Device Manager > Provisioning Templates > SD-WAN Overlay Template*.
2. Create or edit an SD-WAN overlay template.
3. On the *Role Assignment (2/5)* step in the wizard, enable *Automatic Branch ID Assignment*.

The screenshot displays the 'Edit SD-WAN Overlay Template - Role Assignment (2/5)' configuration window. The 'Name' field is set to 'corpa_region'. Under 'Topology', 'Dual HUB (Primary & Primary)' is selected. The 'HUB' section shows two 'Primary HUB' entries, both assigned to 'HUB1' and 'HUB2' respectively. In the 'Branch' section, 'Device Group Assignment' is set to 'grp1'. The 'Automatic Branch ID Assignment' toggle is turned on. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

- When *Automatic Branch ID Assignment* is enabled, FortiManager automatically assigns and tracks a branch ID for each device in the branch device group. This also applies to devices added to the branch device group in the future, as well as those added to the device group using a zero-touch provisioning device blueprint.

- Branch ID values are between one and the maximum number allowed by the subnet. For example, the default 10.10.0.0/255.255.0.0 overlay network uses the /19 subnet when your setup includes 5 - 8 overlays. The maximum allowed branch IDs in this range is 8,190 based on the maximum number of number of usable IPs/FortiGates supported per overlay.

SD-WAN monitoring map integrates with Cloud Assisted Monitoring Service to allow FortiGate interface speed tests from inside FortiManager



This information is also available in the FortiManager 7.4 Administration Guide:

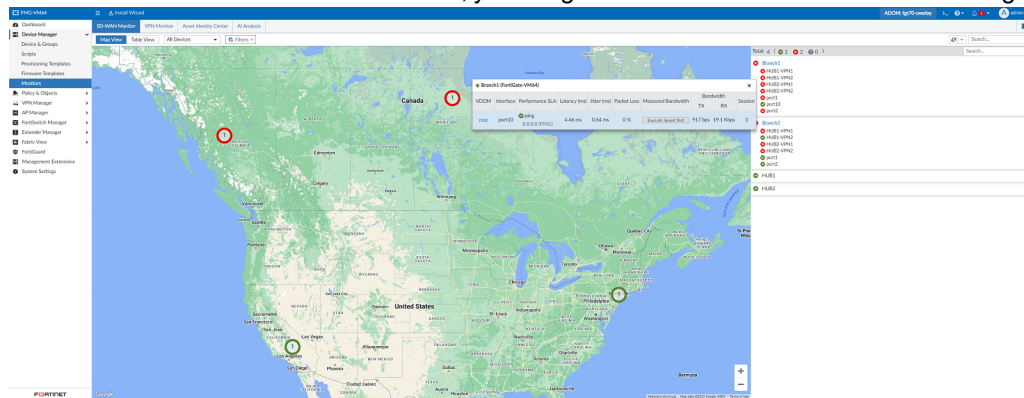
- [SD-WAN Cloud assisted monitoring speed test](#).

SD-WAN Monitoring Map integrates with Cloud Assisted Monitoring Service to allow FortiGate interface speed tests from inside FortiManager.

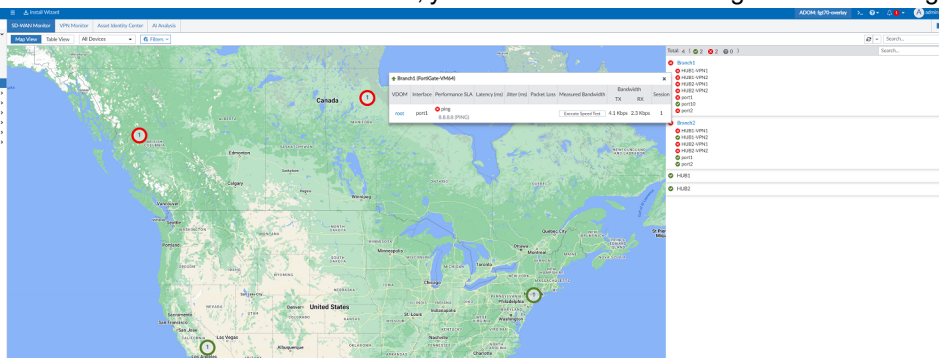
To execute an SD-WAN speed test:

1. Execution of speed tests can be performed from the *SD-WAN Monitor* page: Map View, Table View, Device Drilldown and the Device Dashboard.
2. For devices with a valid license and an interface set with the WAN role, the *Execute Speed Test* option is displayed for the interface.

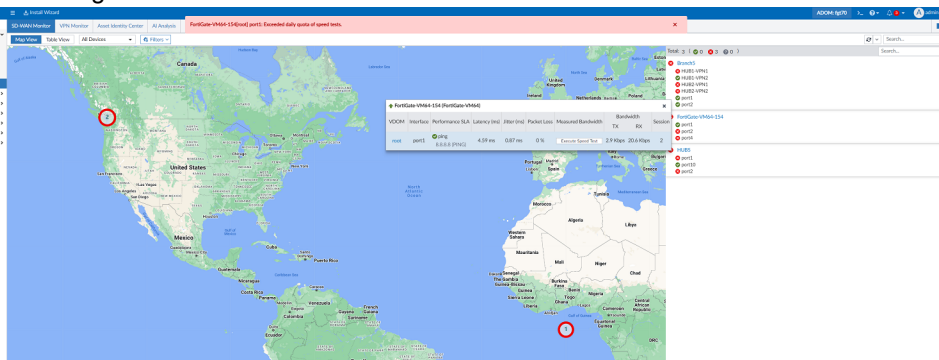
- If there is a valid route to the cloud server, you will get measured bandwidth when executing the speed test.



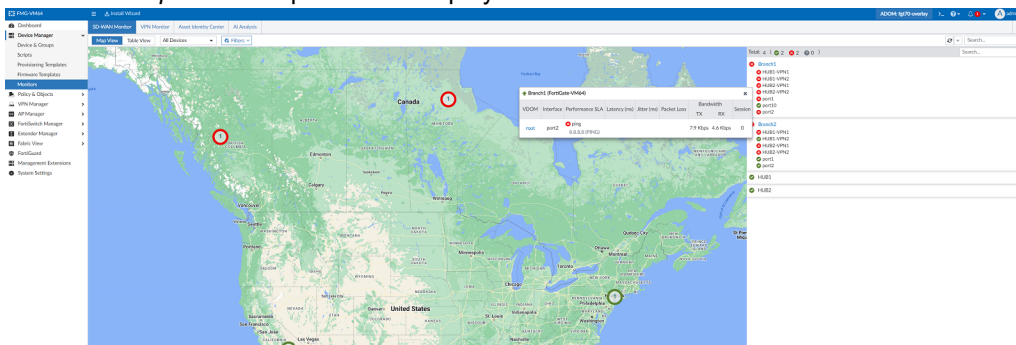
- If there is not a valid route to the cloud server, you will see an error message when executing the speed test.



- You can perform the speed test up to 10 times per day. Attempts to perform additional speed tests will present an error message.



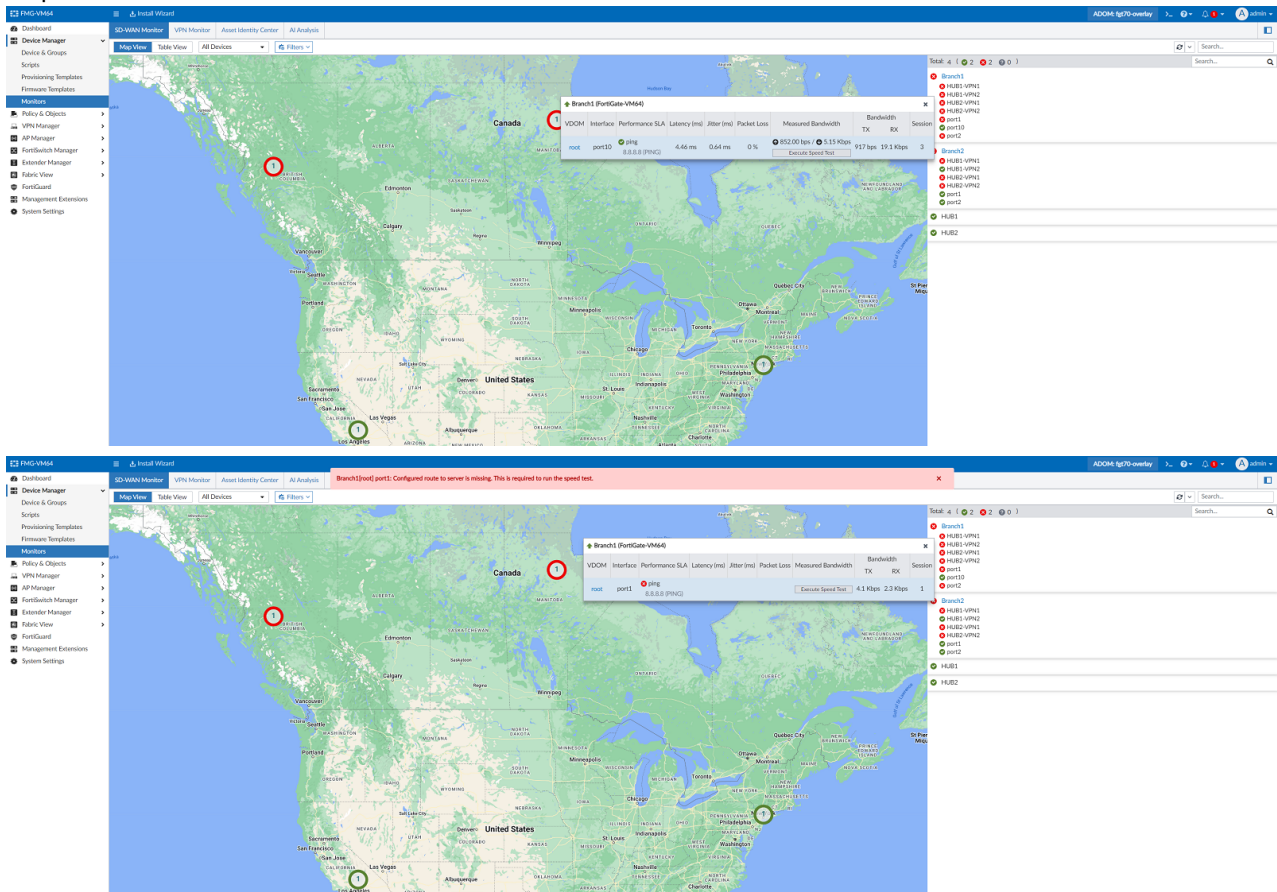
- For devices without a valid license, or for devices with a valid license but without an interface set to the WAN role, the *Execute Speed Test* option is not displayed.



To view the results in SD-WAN Monitor pages:

The latest results of the speed test are displayed on the SD-WAN Monitor pages, including:

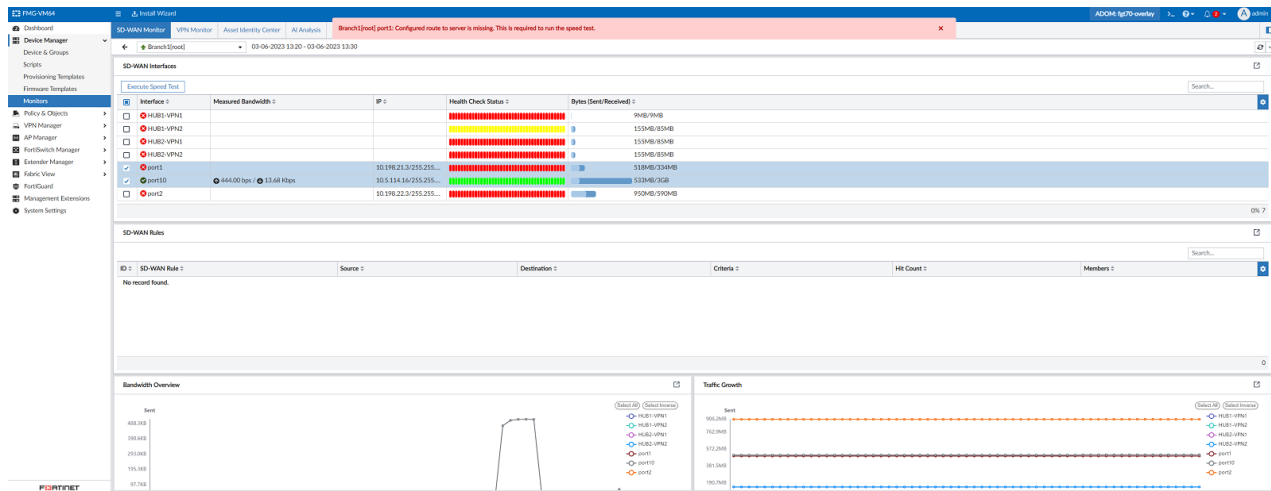
- Map View:



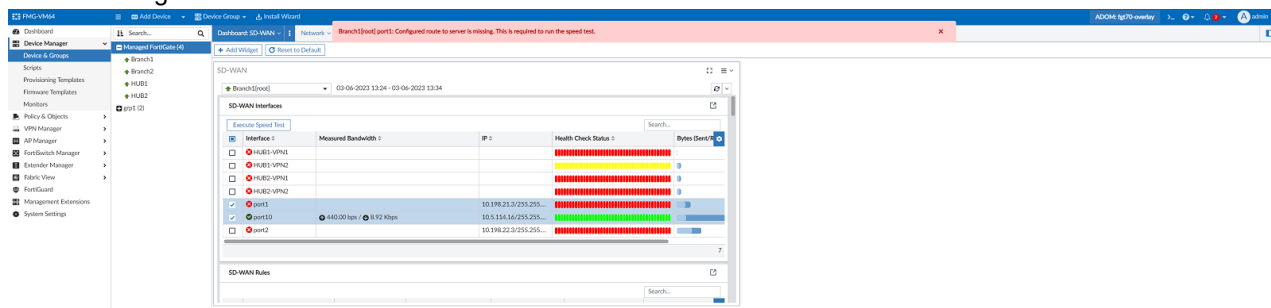
- Table View:

Branch2[port1]: Configured route to server is missing. This is required to run the speed test.										
Device	SD-WAN Interface	Upload	Download	Measured Bandwidth						
Branch1	HUB1-VPN1	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps
	HUB1-VPN2	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps
	HUB2-VPN1	1.3 Kbps/0 tps	0 tps/0 tps	1.3 Kbps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps
	HUB2-VPN2	1.3 Kbps/0 tps	0 tps/0 tps	1.3 Kbps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps
	port1	4.1 Kbps/0 tps	0 tps/0 tps	4.1 Kbps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps
Branch2	HUB1-VPN1	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps
	HUB1-VPN2	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps
	HUB2-VPN1	651 tps/0 tps	0 tps/0 tps	651 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps
	HUB2-VPN2	648 tps/0 tps	0 tps/0 tps	648 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps
	port1	659 tps/0 tps	0 tps/0 tps	659 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps	0 tps/0 tps

- Device Drilldown:



- Device Manager > Device Dashboard > SD-WAN Monitor:



SDWAN monitoring map enhancements



This information is also available in the FortiManager 7.4 Administration Guide:

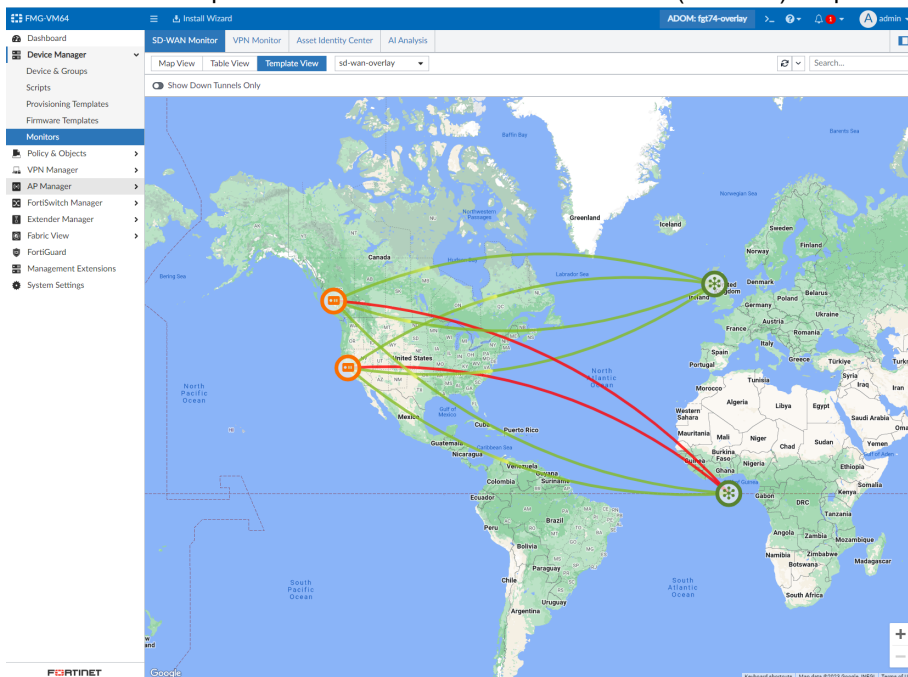
- [Template View](#)

SDWAN monitoring map differentiates HUB and branch device types, displays the overlay connectivity between devices and WAN underlay ports SLA performances.

To monitor SD-WAN with the Template View:

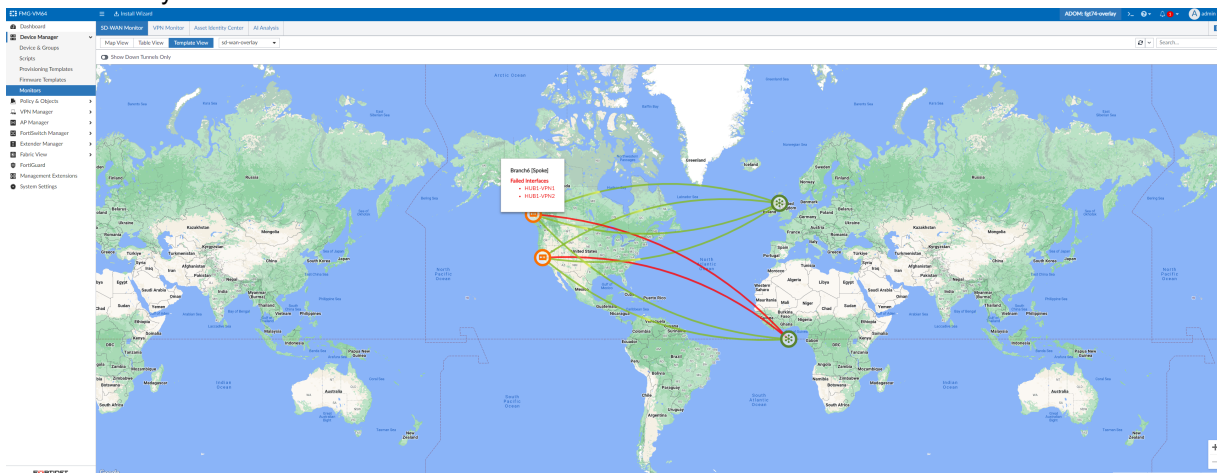
- Go to the *Device Manager > Monitors > SD-WAN Monitor* pane, and click *Template View*.
 - SD-WAN devices provisioned using the currently selected SD-WAN template are displayed on the map.
 - Only devices provisioned using the selected SD-WAN template are displayed. You can change the selected SD-WAN template by clicking the dropdown in the toolbar and selecting a new template.

- Devices on the map are identified with icons as either a HUB (star icon) or spoke device (device icon).

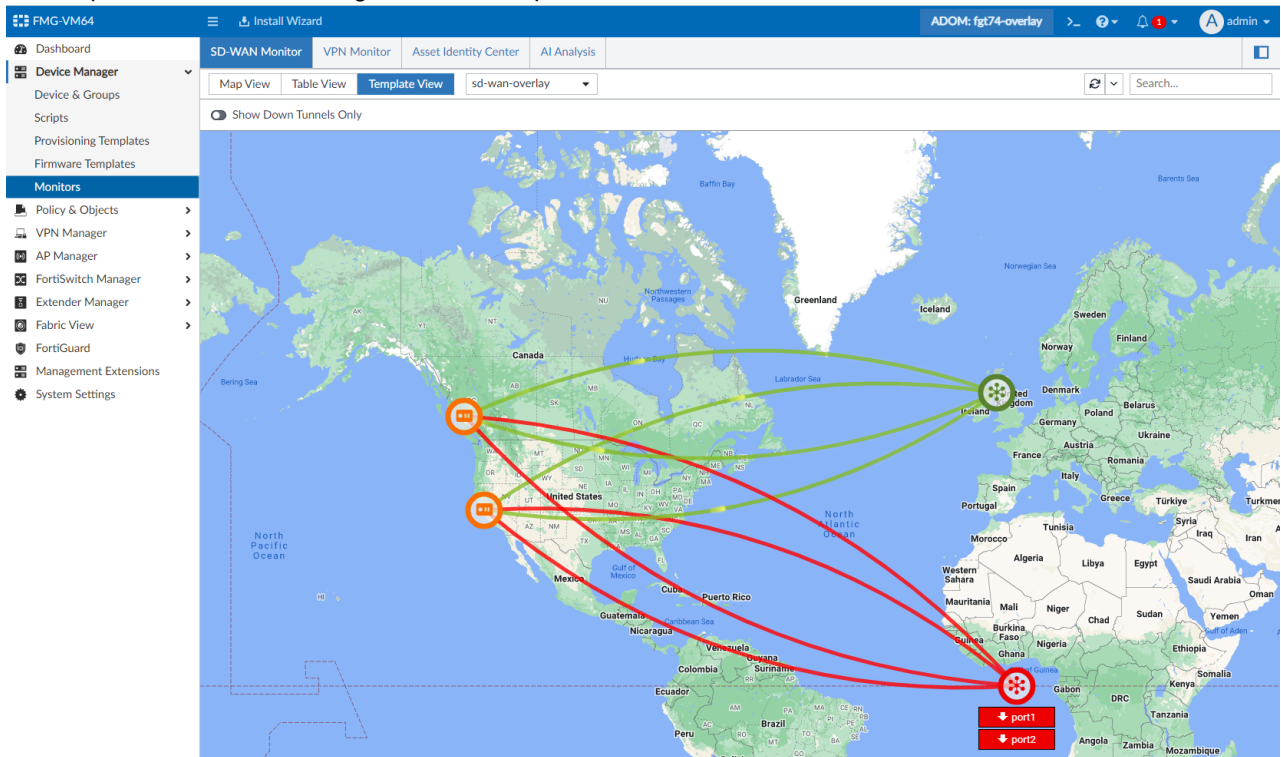


2. Hovering your mouse over a device on the map displays the following information:

- Device name and whether it is a HUB or spoke.
- Interfaces that have a failed health check.
- Down underlays.



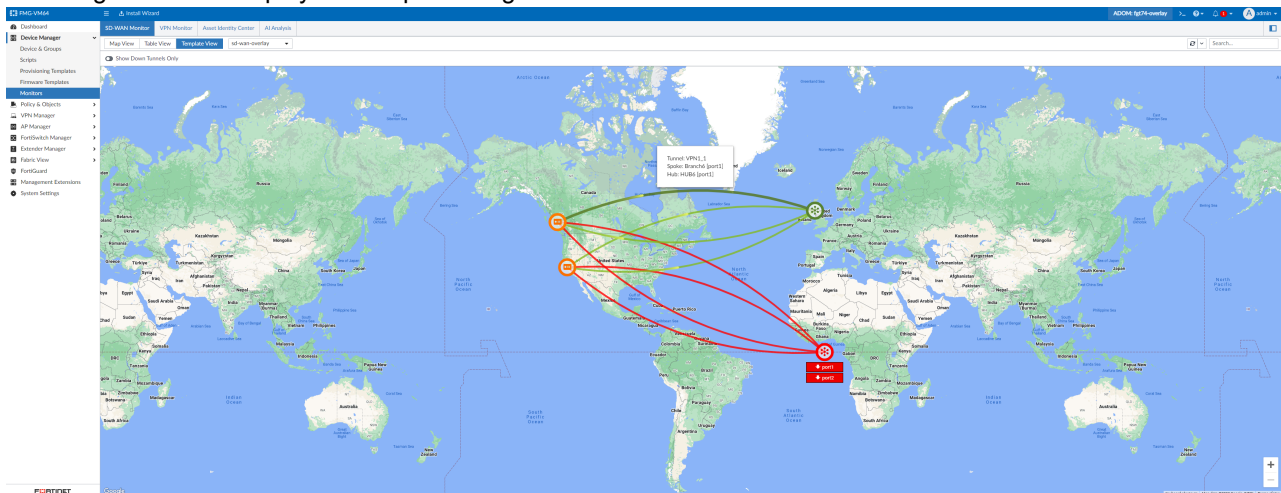
3. The map shows lines connecting the HUB and spoke devices.



The line color depends on if the tunnel is up (green) or down (red). Device color is based off of the following logic:

- a. If the SD-WAN health checks are defined on the device (usually a spoke):
 - Green: All health checks pass.
 - Orange: Some health checks pass.
 - Red: All health checks fail.
- b. When no SD-WAN health checks are defined on the device (usually a HUB):
 - Green: All underlays are up.
 - Orange: Some underlays are up.
 - Red: All underlays are down.

4. Hovering over a line displays a tooltip showing both device names.



5. Clicking on a line opens a pane with the following information:

- Underlay Status table of HUB and spoke devices.
- Health check table for the spoke devices.

The screenshot shows the FortiManager interface with a map view of a network topology. A line is selected, and the right pane displays the configuration for 'VPN_1'. The 'Underlay Interfaces' section shows a table with columns: Name, Status, and Bytes. The 'Overlay Interfaces' section shows a table with columns: Interface, SLA, Latency (ms), Jitter (ms), Packet Loss, Bandwidth, and Bytes (Sent/Received). The 'Health Check' table shows data for HUB and spoke devices.

Interface	SLA	Latency (ms)	Jitter (ms)	Packet Loss	Bandwidth	Bytes (Sent/Received)
HUB1-VPN1	HUB1_HC #1	0.00 / 0.00ms	0.00 / 0.00ms	0.00%	100.00 / 0.00	0.00KB / 0.00KB
HUB2-VPN1	HUB2_HC #1	0.00 / 0.00ms	0.00 / 0.00ms	0.00%	100.00 / 0.00	0.00KB / 0.00KB

6. Clicking on a spoke device opens a pane with the following information.

- SD-WAN health check table.
- Underlay status table.
- IPsec VPN table.
- Routing - Static & Dynamic table.

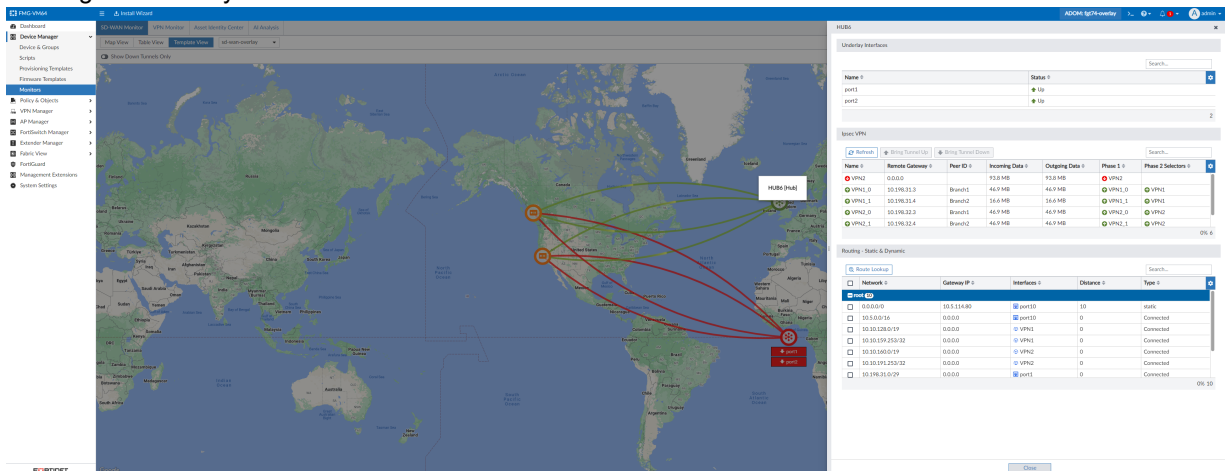
The screenshot shows the FortiManager interface with a map view of a network topology. A spoke device is selected, and the right pane displays the configuration for the spoke device. The 'Underlay Interfaces' section shows a table with columns: Name, Status, and Bytes. The 'Overlay Interfaces' section shows a table with columns: Interface, SLA, Latency (ms), Jitter (ms), Packet Loss, Bandwidth, and Bytes (Sent/Received). The 'Health Check' table shows data for HUB and spoke devices. The 'IPsec VPN' table shows data for IPsec VPNs. The 'Routing - Static & Dynamic' table shows data for static and dynamic routes.

Interface	SLA	Latency (ms)	Jitter (ms)	Packet Loss	Bandwidth	Bytes (Sent/Received)
HUB1-VPN1	HUB1_HC #1	0.00 / 0.00ms	0.00 / 0.00ms	0.00%	100.00 / 0.00	0.00KB / 0.00KB
HUB2-VPN1	HUB2_HC #1	0.00 / 0.00ms	0.00 / 0.00ms	0.00%	100.00 / 0.00	0.00KB / 0.00KB

7. Clicking on a HUB device opens a pane with the following information:

- Underlay Status table.
- IPsec VPN table.

- Routing - Static & Dynamic table.



SDWAN template for heterogeneous WAN link types



This information is also available in the FortiManager 7.4 Administration Guide:

- [Zones and interface members](#)
- [Performance SLA](#)

SDWAN template for heterogeneous WAN link types to support single-template usage for FortiGates with different underlay connections and SLAs.

To create an SD-WAN template with heterogeneous WAN links:

1. Go to *Device Manager > Provisioning Templates > SD-WAN Template*, and create or edit a template.
2. You can select the installation target for the following SD-WAN objects:
 - system sdwan members
 - system sdwan service
 - system sdwan health-check

- system sdwan neighbor

Top Screenshot: Edit SD-WAN Template

Name: SD-WAN-b6552
Description: [Used by SDWAN Overlay Template: sd-wan-overlay]

SD-WAN Status: ☒

Interface Members

ID	Interface Member	Status	Gateway	Cost	Installation Target
	virtual-wan-link				1 Device in Total View Details >
3	port3	Enable	0.0.0.0	0	FG-VM64-146 [root]
4	port4	Enable	0.0.0.0	0	FG-VM64-147 [root]
5	port5	Enable	0.0.0.0	0	Branch5 [root]
WAN1	port1	Enable	0.0.0.0	0	

0% 9

Bottom Screenshot: Edit SD-WAN Member

Sequence Number: 3
Interface Member: port3
SD-WAN Zone: virtual-wan-link
Gateway IP: 0.0.0.0
Cost: 0
Status: ☒
Priority: 1
Installation Target: FG-VM64-146 [root] (1 entry selected)

Advanced Options >

3. You can add meta variables for the following health-check attributes:

- System SD-WAN health-check
 - Check Interval
 - Fail Before Inactive
 - Probe Timeout
 - Restore Link After
- System SD-WAN health-check SLA
 - Link Cost Factor
 - Latency Threshold
 - Jitter Threshold
 - Packet Loss Threshold

- Mos Threshold

The screenshot displays the FortiManager 7.4.0 interface. On the left, the 'Device Manager' menu is open, showing 'Provisioning Templates' as the active section. The main window is titled 'Edit Performance SLA'. It contains several configuration fields: 'Name' (ping1), 'IP Version' (IPv4), 'Probe Mode' (Active), 'Enable Probe Packets' (checked), 'Protocol' (Ping), 'Server' (8.8.8.8), 'Participants' (All SD-WAN Members), 'Embedded Measure Health' (checked), 'Redistribute SLA ID' (0), and 'Installation Target' (FG-VM64-146 [root]). Below these fields is the 'SLA Target' table, which has columns for Link Cost Factor, Latency Threshold, Jitter Threshold, Packet Loss Threshold, Mos Threshold, Priority IN-SLA, and Priority OUT-SLA. The 'Link Status' section includes fields for Check Interval (500s), Failure Before Inactive (5s), Restore Link After (5s), and Probe Timeout (500s). The 'Action When Inactive' section includes fields for Update Static Route (checked) and Cascade Interfaces (checked). At the bottom, there are 'OK' and 'Cancel' buttons.

Templates

This section lists the new features added to FortiManager for templates:

- [Preview CLI configuration for the device provisioning templates on page 25](#)
- [Fortinet factory-default wireless and extender templates on page 28](#)
- [Jinja Templates have direct access to the device DB to support generation of dynamic configuration on page 34](#)
- [Fabric Authorization Template is integrated with Device Blueprint and supports meta variables 7.4.1 on page 41](#)

Preview CLI configuration for the device provisioning templates



This information is also available in the FortiManager 7.4 Administration Guide:

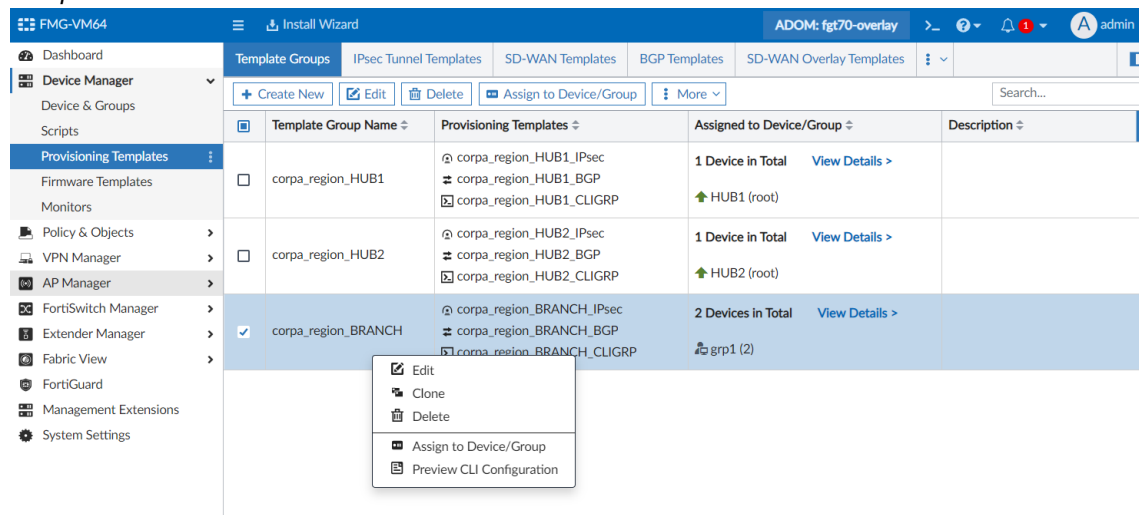
- [Viewing the CLI preview for provisioning templates](#)

In FortiManager, you can preview the CLI configuration for the device provisioning templates.

To preview the CLI configuration for provisioning templates:

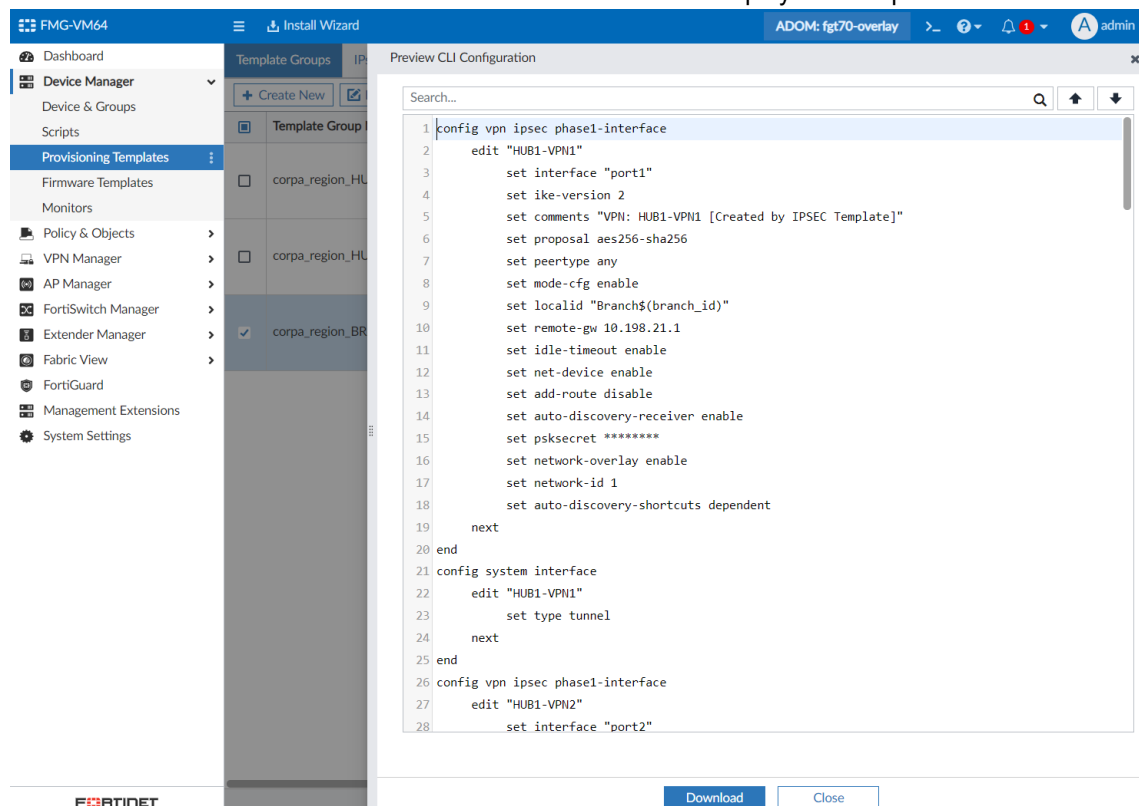
1. Go to *Device Manager > Provisioning Templates*.
Select a template type by choosing the corresponding tab. You can view the CLI preview for all provisioning template types, including: *Template Groups*, *IPsec Tunnel Templates*, *SD-WAN Templates*, *BGP Templates*, *SD-*

WAN Overlay Templates, System Templates, Static Route Templates, CLI Templates, and Threat Weight Templates.



- Right-click on a template, and choose *Preview CLI Configuration*.

The *Preview CLI Configuration* window is displayed with the CLI configuration for the selected template. The metadata variable names and not their resolved values are displayed in the preview.



- When the provisioning template includes multiple devices, you can select a device from the *Device* dropdown. The CLI preview for the selected device is displayed in the content pane.

The screenshot displays the FortiManager 7.4.0 interface. The top navigation bar shows the user is logged in as 'admin' and the current view is 'ADOM: fgt70-overlay'. The left sidebar contains the 'Device Manager' menu, with 'Provisioning Templates' selected. The main table lists templates, with the first entry 'corpa_region' selected. A context menu is open over this entry, showing options: Edit, Clone, Delete, and Preview CLI Configuration. The 'Preview CLI Configuration' window is open, showing the CLI configuration for the selected template. The configuration is for a VPN phase1-interface named 'HUB1-VPN1' and is applied to the device group 'grp1'.

#	Template Name	Topology	Assign to Device/Group	Loopback IP Address	Overlay Network
1	corpa_region	Dual HUB (Primary & Primary)	HUB1 HUB2 grp1	172.16.0.0/255.255.0.0	10.10.0.0/255.255.0.0

```
1 config vpn ipsec phase1-interface
2   edit "HUB1-VPN1"
3     set interface "port1"
4     set ike-version 2
5     set comments "VPN: HUB1-VPN1 [Created by IPSEC Template]"
6     set proposal aes256-sha256
7     set peertype any
8     set mode-cfg enable
9     set localid "Branch$(branch_id)"
10    set remote-gw 10.198.21.1
11    set idle-timeout enable
12    set net-device enable
13    set add-route disable
14    set auto-discovery-receiver enable
15    set psksecret *****
16    set network-overlay enable
17    set network-id 1
18    set auto-discovery-shortcuts dependent
19  next
20 end
21 config system interface
22   edit "HUB1-VPN1"
23     set type tunnel
24  next
```


4. In the *Preview CLI Configuration* window, you can search in the CLI using the search bar, and you can download the CLI preview by clicking the *Download* button.

The screenshot shows the FortiManager interface with the 'Preview CLI Configuration' window open. The window displays the CLI configuration for a VPN interface. The configuration lines are as follows:

```

1 config vpn ipsec phase1-interface
2   edit "HUB1-VPN1"
3     set interface "port1"
4     set ike-version 2
5     set comments "VPN: HUB1-VPN1 [Created by IPSEC Template]"
6     set proposal aes256-sha256
7     set peertype any
8     set mode-cfg enable
9     set localid "Branch$(branch_id)"
10    set remote-gw 10.198.21.1
11    set idle-timeout enable
12    set net-device enable
13    set add-route disable
14    set auto-discovery-receiver enable
15    set psksecret *****
16    set network-overlay enable
17    set network-id 1
18    set auto-discovery-shortcuts dependent
19  next
20 end
21 config system interface
22   edit "HUB1-VPN1"
23     set type tunnel
24  next
  
```

At the bottom of the window, there are buttons for 'Download' and 'Close'.

Fortinet factory-default wireless and extender templates

FortiManager includes Fortinet factory-default wireless and extender templates with built-in security and network configuration based on best security practices.






This information is also available in the FortiManager 7.4 Administration Guide:

- [Using Fortinet recommended FortiAP and SSID profiles](#)
- [Using Fortinet recommended extender profiles](#)

To use default FortiAP profiles and SSIDs:

- Recommended FortiAP profiles are available in the FortiManager *AP Manager*.
 - Go to *AP Manager > Operation Profiles* under the *FortiAP Profiles* tab.

<div><div><div><div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div><div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div><div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div></div><div><div>Create New</div><div>Edit</div><div>Delete</div><div>More</div></div></div><div><div>View All Profiles</div><div>Search...</div></div></div>						
<input type="checkbox"/>	Name	Platform	Radio Mode	Bands	SSIDs	Comment
AP Profiles Fortinet Recommended - Factory Default (3)						
<input type="checkbox"/>	 Corporate_Fortinet_Default		R1: Access Point R2: Access Point	R1: N/A R2: N/A	R1: All Tunnel Mode SSIDs R2: All Tunnel Mode SSIDs	Fortinet Recommended profile for Corporate
<input type="checkbox"/>	 Guest_Fortinet_Default		R1: Access Point R2: Access Point	R1: N/A R2: N/A	R1: All Tunnel Mode SSIDs R2: All Tunnel Mode SSIDs	Fortinet Recommended profile for Guest
<input type="checkbox"/>	 POS_Fortinet_Default		R1: Access Point R2: Access Point	R1: N/A R2: N/A	R1: All Tunnel Mode SSIDs R2: All Tunnel Mode SSIDs	Fortinet Recommended profile for POS
AP Profiles (1)						
<input type="checkbox"/>	FAP24D-default	FAP24D	R1: Access Point	R1: 2.4GHz 802.11n/g	R1: ss11	

- b. Right click on a recommended AP profile and click **View**.

The screenshot shows the FortiManager Device Manager interface. At the top, there are buttons for '+ Create New', 'View', 'Delete', and 'More'. Below these is a table of AP Profiles. The table has columns: Name, Platform, Radio Mode, Bands, SSIDs, and Comment. There are two sections: 'AP Profiles Fortinet Recommended - Factory Default (3)' and 'AP Profiles (1)'. In the first section, the 'Corporate_Fortinet_Default' profile is selected, and a right-click context menu is open with 'View' highlighted. In the second section, the 'FAP24D-default' profile is listed. Below the table, the 'View AP Profile' dialog is open for the 'Corporate_Fortinet_Default' profile. The dialog shows fields for Name, Comments, Platform (FAP221E), Country/Region (Use default), FortiAP Configuration Profile (Set), AP Login Password (Set), Administrative Access (HTTPS, SNMP, SSH), Client Load Balancing, Bluetooth Profile, and Radio 1 settings (Mode: Access Point, WIDS Profile, Radio Resource Provision, Band: 2.4 GHz, Channel Width: 40MHz, Channel Plan: Custom, Channels: 1-6, Short Guard Interval, Transmit Power Mode: Percent).

2. FortiAP profiles based on the recommended profiles can be created by activating the recommended profiles.

- a. Right-click on a recommended profile and click **Activate**.

This screenshot is similar to the previous one, showing the FortiManager Device Manager interface. The 'Corporate_Fortinet_Default' profile is selected, and a right-click context menu is open. In this instance, the 'Activate' option is highlighted in the menu. The 'AP Profiles (1)' section still shows the 'FAP24D-default' profile.

- b. Select the platform type for the profile.

This screenshot shows the 'Choose Template Platform' dialog box open over the FortiManager Device Manager interface. The dialog has a 'Platform' dropdown menu and a list of available platforms. The platforms are categorized into 'Existing AP Platforms' (FAP24D) and 'Other Platforms' (FAP112B, FAP112D, FAP11C, FAP14C). The 'FAP24D' platform is currently selected in the dropdown.

- c. Enter a name for the AP profile and configure the remaining settings if required.

AP Profile

Name: 24d-default

Comments:

Platform: FAP24D

Indoor / Outdoor: Default (Indoor) Indoor Outdoor

Country / Region: Use default

FortiAP Configuration Profile

AP Login Password: Set Leave Unchanged Set Empty

Administrative Access: ☒ HTTPS ☒ SNMP ☒ SSH

Client Load Balancing: ☐ Frequency Handoff ☐ AP Handoff

Radio 1

Mode: Disabled Access Point Dedicated Monitor SAM Packet Sniffer

WIDS Profile: Disabled

Radio Resource Provision: arp-default

Band: 2.4 GHz 5 GHz 802.11n/g/b

Channel Width: 20MHz 40MHz

Channel Plan: Three Channels Four Channels Custom

Channels: ☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☒ 11

Short Guard Interval: Disabled

Transmit Power Mode: Percent

OK Cancel

3. The recommended default AP SSIDs are shown in *AP Manager > SSIDs*.

- a. Go to *FortiAP > SSIDs* to view the default SSIDs.

+ Create New Edit Delete More							Search...
<input type="checkbox"/>	Name	SSID	Traffic Mode	Security Mode	Schedule	Data Encryption	Maximum Clients
SSIDs Fortinet Recommended - Factory Default (3)							
<input type="checkbox"/>	Corporate_Fortinet_Default	Corporate	Local Bridge	WPA2 Enterprise	Always	AES	0
<input type="checkbox"/>	Guest_Fortinet_Default	Guest	Tunnel	Captive Portal	Always		0
<input type="checkbox"/>	POS_Fortinet_Default	POS	Local Bridge	WPA2 Personal	Always	AES	0
SSIDs (1)							
<input type="checkbox"/>	ss11	ss11	Tunnel	WPA2 Personal	Always	AES	0
SSID Groups (0)							

- b. Right click on a recommended SSID and click **View** to view its details.

The screenshot shows the FortiManager Device Manager interface. At the top, there's a toolbar with 'Create New', 'View', 'Delete', and 'More' buttons. Below it is a table of SSIDs. The table has columns: Name, SSID, Traffic Mode, Security Mode, Schedule, Data Encryption, and Maximum Clients. The table is divided into sections: 'SSIDs Fortinet Recommended - Factory Default (3)', 'SSIDs (1)', and 'SSID Groups (0)'. The 'Corporate_Fortinet_Default' SSID is selected, and a context menu is open with options: View, Clone, Delete, Where Used, and Activate. The 'View' option is highlighted. Below the table, the 'View SSID' dialog is open, showing the configuration for 'Corporate_Fortinet_Default'. The dialog has fields for Name, Alias, Traffic Mode (set to Bridge), and a 'WiFi Settings' section. The 'WiFi Settings' section includes SSID (Corporate), Security Mode (WPA2 Enterprise), PMF (Disable, Enable, Optional), Local Standalone, Local Authentication, Client Limit, Authentication (Local, RADIUS Server), Broadcast SSID, Dynamic VLAN Assignment, and Schedule (always, Start:00:00-End:00:00 SMTWTFS). The 'Return' button is at the bottom.

Name	SSID	Traffic Mode	Security Mode	Schedule	Data Encryption	Maximum Clients
SSIDs Fortinet Recommended - Factory Default (3)						
<input checked="" type="checkbox"/> Corporate_Fortinet_Default	Corporate	Local Bridge	WPA2 Enterprise	Always	AES	0
<input type="checkbox"/> Guest_Fortinet_Default	Guest	Tunnel	Captive Portal	Always		0
<input type="checkbox"/> POS_Fortinet_Default	POS	Local Bridge	WPA2 Personal	Always	AES	0
SSIDs (1)						
<input type="checkbox"/> ss11	ss11	Tunnel	WPA2 Personal	Always	AES	0
SSID Groups (0)						

View SSID

Name: Corporate_Fortinet_Default

Alias:

Traffic Mode: Bridge

WiFi Settings

SSID: Corporate

Security Mode: WPA2 Enterprise

PMF: Disable Enable Optional

Local Standalone:

Local Authentication:

Client Limit:

Authentication: Local RADIUS Server

Broadcast SSID:

Dynamic VLAN Assignment:

Schedule: always Start:00:00-End:00:00 SMTWTFS

Block Intra-SSID Traffic:

Optional VLAN ID: 0

Broadcast Suppression:

Return

4. An SSID can be created by activating the recommended SSIDs.

- a. Right-click on a recommended SSID and click **Activate**.

This screenshot is similar to the previous one, showing the FortiManager Device Manager interface. The 'Corporate_Fortinet_Default' SSID is selected, and the context menu is open. The 'Activate' option is highlighted with a red box.

Name	SSID	Traffic Mode	Security Mode	Schedule	Data Encryption	Maximum Clients
SSIDs Fortinet Recommended - Factory Default (3)						
<input checked="" type="checkbox"/> Corporate_Fortinet_Default	Corporate	Local Bridge	WPA2 Enterprise	Always	AES	0
<input type="checkbox"/> Guest_Fortinet_Default	Guest	Tunnel	Captive Portal	Always		0
<input type="checkbox"/> POS_Fortinet_Default	POS	Local Bridge	WPA2 Personal	Always	AES	0
SSIDs (1)						
<input type="checkbox"/> ss11	ss11	Tunnel	WPA2 Personal	Always	AES	0
SSID Groups (0)						

View SSID

Name: Corporate_Fortinet_Default

Alias:

Traffic Mode: Bridge

WiFi Settings

SSID: Corporate

Security Mode: WPA2 Enterprise

PMF: Disable Enable Optional

Local Standalone:

Local Authentication:

Client Limit:

Authentication: Local RADIUS Server

Broadcast SSID:

Dynamic VLAN Assignment:

Schedule: always Start:00:00-End:00:00 SMTWTFS

Block Intra-SSID Traffic:

Optional VLAN ID: 0

Broadcast Suppression:

Return

- b. Enter a name for the SSID and configure the remaining settings as needed.

The screenshot shows the 'SSID' configuration window. The 'Name' field is set to 'ssid22'. The 'Alias' field is also 'ssid22'. The 'Traffic Mode' is set to 'Bridge'. Under 'WiFi Settings', the 'SSID' is 'Corporate', 'Security Mode' is 'WPA2 Enterprise', and 'PMF' is set to 'Enable'. The 'Authentication' section shows 'Local' and 'RADIUS Server' tabs, with 'RADIUS Server' selected. The 'Broadcast SSID' is set to 'On'. The 'Dynamic VLAN Assignment' section shows a search bar and a list of entries, with 'always' selected. The 'Block Intra-SSID Traffic' is set to 'On'. The 'Optional VLAN ID' is set to '0'. The 'Broadcast Suppression' is set to 'On'. The 'OK' and 'Cancel' buttons are at the bottom.

5. The created SSID can be assigned to an AP profile, and the profile can be assigned to the FortiAP.
- a. In the FortiAP Profile, select the configured SSID.

The screenshot shows the 'Edit AP Profile' window. The 'Transmit Power' section shows 'dBm' selected, with a slider set to 27 dBm. The 'SSID' section shows 'Manual' selected, with a search bar and a list of entries. The 'Selected 1 (Total: 3)' list shows 'ssid22' selected. The 'Monitor Channel Utilization' is set to 'On'. The 'Advanced Options' section is expanded, showing 'System Log', 'Syslog Profile', 'LAN Configuration', 'ESL SES Dongle Configuration', 'APC FQDN', 'Location Based Services', and 'FortiPresence'. The 'OK' and 'Cancel' buttons are at the bottom.

b. Assign the profile to the FortiAP device.

The screenshot shows the FortiManager Device Manager interface. On the left, a sidebar lists managed devices: Managed FortiGate (3), FGVM_MODEL, FGVM_MODEL_OLD, FortiGate-140E-POE (3), and FortiGate-400E. The main area displays a summary of 3 total devices, all online. Below this, a table lists access points. A context menu is open for the first device (FAP24D3X17005555), showing options like Authorize, Deauthorize, Upgrade, Restart, Refresh, Register, Assign Profile, Diagnostics and Tools, LED Blink, Show on Google Map, Show on Floor Map, Replace, and Grouping. The 'Assign Profile' option is highlighted, and a dropdown menu shows '24d-default' and 'FAP24D-default'.

Access Point	Status	SSIDs	Channel	Clients	Temperature	OS Version	AP Profile	Connected Via	Model	Channel Utilization	FortiAP Group
FAP24D3X17005555	Online	N/A	N/A	R1: 0		FAP24D-v6.0-build0044		192.168.100.111	24D	28	
FAP24D3X1600			N/A	R1: 0		FAP24D-v6.0-build0044		192.168.100.113	24D	0	
FAP24D3X1600			N/A	R1: 0		FAP24D-v6.0-build0044		192.168.100.112	24D	46	

To use recommended FortiExtender templates:

1. The recommended Extender Profile is shown in *Extender Manager > Extender Profiles*.

The screenshot shows the FortiManager Extender Manager > Extender Profiles interface. It displays a table of extender profiles. The 'Factory Default FortiExtender (1)' profile is highlighted with a red box. Below it, the 'Fortinet_Default_FEXT_Profile' is listed. Under the 'Extension Controller (3)' section, three profiles are shown: 201lan, 201wan, and FX201E_wanext.

Title	Model	Mode	Assigned FortiExtender
Factory Default FortiExtender (1)			
Fortinet_Default_FEXT_Profile		WAN Extension	
Extension Controller (3)			
201lan	FX201E	LAN Extension	
201wan	FX201E	WAN Extension	
FX201E_wanext	FX201E	WAN Extension	FortiGate-140E-POE [root] - FX0015920007745

2. An extender profile can be created by activating the recommended FortiExtender profile.

a. Right-click on the recommended FortiExtender profile and click *Activate*.

The screenshot shows the FortiManager Extender Manager > Extender Profiles interface. A context menu is open for the 'Fortinet_Default_FEXT_Profile' entry, showing options like View, Clone, Delete, Assign to Device, Where Used, and Activate. The 'Activate' option is highlighted with a red box.

Title	Model	Mode	Assigned FortiExtender
Factory Default FortiExtender (1)			
Fortinet_Default_FEXT_Profile		WAN Extension	
Extension Controller (3)			
201lan	FX201E	LAN Extension	
201wan	FX201E	WAN Extension	
FX201E_wanext	FX201E	WAN Extension	FortiGate-140E-POE [root] - FX0015920007745

b. Choose a model for the template.

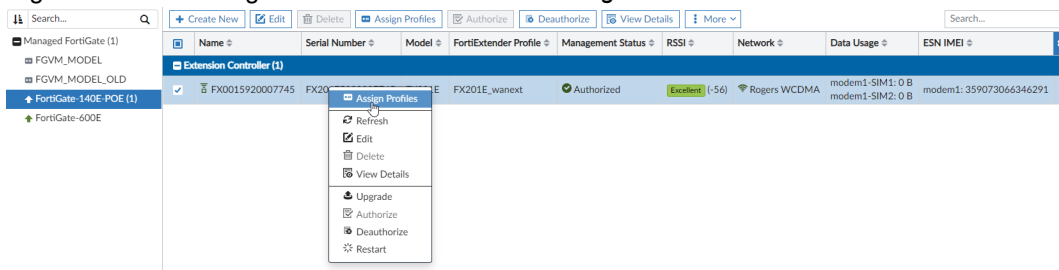
The screenshot shows the FortiManager Extender Manager > Extender Profiles interface. A 'Choose Template Model' dialog box is open, displaying a list of models. The 'FX201E' model is selected and highlighted in blue.

Title	Model	Mode	Assigned FortiExtender
Factory Default FortiExtender (1)			
Fortinet_Default_FEXT_Profile		WAN Extension	
Extension Controller (3)			
201lan	FX201E	LAN Extension	
201wan	FX201E	WAN Extension	
FX201E_wanext	FX201E	WAN Extension	FortiGate-140E-POE [root] - FX0015920007745

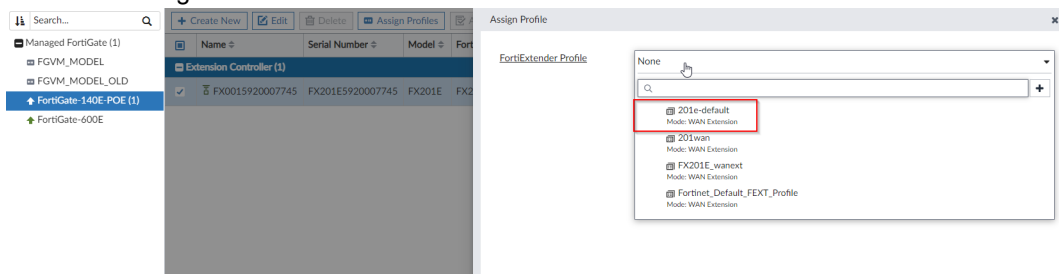
- c. Enter a name for the FortiExtender profile and configure the remaining settings as needed.

3. The created extender profile can be assigned to an extender, then the user can deploy the settings.

- a. Right-click on a managed FortiExtender and click *Assign Profiles*.



- b. Select the configured FortiExtender Profile.



Jinja Templates have direct access to the device DB to support generation of dynamic configuration



This information is also available in the FortiManager 7.4 Administration Guide:

- [Using FortiManager device database variables in Jinja](#)

Jinja Templates have direct access to the device database to support generation of dynamic configuration.

The following FortiManager variables are supported:

Supported Device Database Variables	Supported System Interface Variables
<ul style="list-style-type: none"> • Name: <code>{{DVMDB.name}}</code> • Serial: <code>{{DVMDB.serial}}</code> • OS TYPE: <code>{{DVMDB.os_type}}</code> • Platform: <code>{{DVMDB.platform}}</code> • Version: <code>{{DVMDB.version}}</code> • Hostname: <code>{{DVMDB.hostname}}</code> • UUID: <code>{{DVMDB.mgmt_uuid}}</code> • Mgmt Interface IP: <code>{{DVMDB.mgmt_if}}</code> • IP: <code>{{DVMDB.ip}}</code> • Tunnel IP: <code>{{DVMDB.tunnel_ip}}</code> • Description: <code>{{DVMDB.description}}</code> 	<ul style="list-style-type: none"> • Interface Name: <code>{{intf.name}}</code> • Interface Allowaccess: <code>{{intf.allowaccess}}</code> • Interface Type: <code>{{intf.type}}</code> • Interface IP: <code>{{intf.ip}}</code> • Interface Mode: <code>{{intf.mode}}</code> • Interface VDOM: <code>{{intf.vdom}}</code>

This topic includes the following:

- [To use device database variables in a Jinja template: on page 35](#)
- [Example 1: Creating physical interfaces for FortiGate-VMs on page 37](#)
- [Example 2: View the device attributes for FortiGate-VMs on page 39](#)
- [Example 3: View the interface attributes for each physical interface on a device on page 40](#)

To use device database variables in a Jinja template:

1. Go to *Device Manager > Provisioning Templates > CLI Template*.
2. Create a new CLI template.
3. Select the *Type* as *Jinja Script*.
4. Configure the *Script Details* with FortiManager variables. For example, you can use *DVMDB.name* as a variable to get the device name from the Device Database:

```
config system global
set hostname {{DVMDB.name}}
end
```

Edit CLI Template

Template Name

hostname-jinja

Type

Jinja Script

Description

Script Details

Search...

Q

↑

↓

1

config system global

2

set hostname {{DVMDB.name}}

3

end

4

5

6

7

8

9

OK

Cancel

When viewing the *Install Preview* for the CLI Template, the variable *DVMDB.name* is replaced with the *Name* value for the selected device.

Install Preview of vlan171_0070

Assigned Devices

vlan171_0070

vlan171_0070

Search...

Q

↑

↓

1

config system global

2

set hostname "vlan171_0070"

3

end

4

Download

Close

Example 1: Creating physical interfaces for FortiGate-VMs

A user is setting up a FGT-VM64 model device on FortiManager. When setting up a FortiGate-VM, the user needs to execute a script to create the physical interfaces, however, when deploying a FortiGate hardware platform, generating physical interfaces is not necessary. Previously, the user needed to create a separate device group for their FortiGate-VM devices and then runs a script to create the physical interfaces for VM devices inside the device group.

Using Jinja, the same CLI template can be applied to ANY new devices (hardware or VM-based) by using a script with FortiManager variables to determine the platform of the device and using an "if" statement to ensure that the script runs only on FortiGate-VM devices.

Example script:

```
{% if 'FortiGate-VM64' in DVMDB.platform -%}
config system interface
{%- for i in range(0, vm_interface_number|int) %}
edit port{{i+1}}
set vdom root
set type physical
next
{%- endfor %}
end
{%- endif %}
```

Edit Pre-Run CLI Template

Template Name

pre-vm_interface_number

Type

Jinja Script

Description

Script Details

Search...

1 {% if 'FortiGate-VM64' in DVMDB.platform -%}

2

3 config system interface

4 {%- for i in range(0, vm_interface_number|int) %}

5 edit port{{i+1}}

6 set vdom root

7 set type physical

8 next

9 {%- endfor %}

10 end

11

12 {%- endif %}

Revert All Changes

OK

Cancel

Previewing the script on a device shows how the variables are applied.

Preview CLI Template - Preview on Device (3/3)

Assigned Devices

Branch1 [global]

Branch1 [global]

Search...

1

2 config system interface

3 edit port1

4 set vdom root

5 set type physical

6 next

7 edit port2

8 set vdom root

9 set type physical

10 next

11 edit port3

12 set vdom root

13 set type physical

14 next

15 edit port4

16 set vdom root

17 set type physical

18 next

19 edit port5

20 set vdom root

Show Diff View

Download

Close

Example 2: View the device attributes for FortiGate-VMs

Example script:

```
{%- if DVMDB.platform == 'FortiGate-VM64' %}
Name: {{DVMDB.name}}
Serial: {{DVMDB.serial}}
OS TYPE: {{DVMDB.os_type}}
Platform: {{DVMDB.platform}}
Version: {{DVMDB.version}}
hostname: {{DVMDB.hostname}}
UUID: {{DVMDB.mgmt_uuid}}
Mgmt Interface IP : {{DVMDB.mgmt_if}}
IP: {{DVMDB.ip}}
Tunnel IP : {{DVMDB.tunnel_ip}}
Description: {{DVMDB.description}}
```

```
os_type: {{DVMDB.os_type}}
{% - endif %}
```

The rendered result for the script:

```
=====
Name: vlan171_0040
Serial: FGVM08HZ20311040
OS TYPE: FortiGate
Platform: FortiGate-VM64
Version: 7.4.0
hostname: 3456-abc
UUID: 9c50812a-caa8-51ed-958a-4e7800e5139a
Mgmt Interface IP : port1
IP: 10.8.71.40
Tunnel IP : 169.254.0.12
Description:
os_type: FortiGate
```

Example 3: View the interface attributes for each physical interface on a device

Example script:

```
{%- for intf in DEVDB_system_interface %}
{% - if intf.type == 'physical' %}
Interface Name: {{intf.name}}
-- Interface Allowaccess: {{intf.allowaccess}}
-- Interface Type: {{intf.type}}
-- Interface IP: {{intf.ip}}
-- Interface Mode: {{intf.mode}}
-- Interface VDOM: {{intf.vdom}}
{% - endif %}
{% - endfor %}
```

The rendered result for the script:

```
=====
Interface Name: port1
-- Interface Allowaccess: ping
-- Interface Type: physical
-- Interface IP: 10.8.71.40
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port2
-- Interface Allowaccess: https
-- Interface Type: physical
-- Interface IP: 101.71.40.1
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port3
-- Interface Allowaccess: ping
-- Interface Type: physical
-- Interface IP: 200.71.40.1
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port4
-- Interface Allowaccess:
-- Interface Type: physical
```

```
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port5
-- Interface Allowaccess: ping
-- Interface Type: physical
-- Interface IP: 172.71.40.1
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port6
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port7
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port8
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port9
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
Interface Name: port10
-- Interface Allowaccess:
-- Interface Type: physical
-- Interface IP: 0.0.0.0
-- Interface Mode: static
-- Interface VDOM: "root"
```

Fabric Authorization Template is integrated with Device Blueprint and supports meta variables - 7.4.1



This information is also available in the FortiManager 7.4 Administration Guide:

- [Using Device Blueprints for Model Devices](#)
- [Fabric Authorization Templates](#)

In FortiManager 7.4.1, the Fabric Authorization Template is integrated with Device Blueprints and supports metadata variables.

To use Fabric Authorization Templates with Device Blueprints:

- [Step 1: Configure the Fabric Authorization Template on page 42](#)
- [Step 2: Add a Fabric Authorization Template to a device blueprint on page 43](#)
- [Step 3: Add the device blueprint to a model device on page 44](#)
- [Step 4: View the configured FortiAP, FortiSwitch, and FortiExtender on page 44](#)

Step 1: Configure the Fabric Authorization Template

To create a Fabric Authorization Template:

1. Go to *Device Manager > Provisioning Templates > Fabric Authorization*.
2. Click *Create New*, and the *Create New Fabric Authorization Template* dialog appears.
3. Configure the Fabric Authorization Template, for example a template named "60E" is configured in the with the following settings:
 - a. FortiAP:

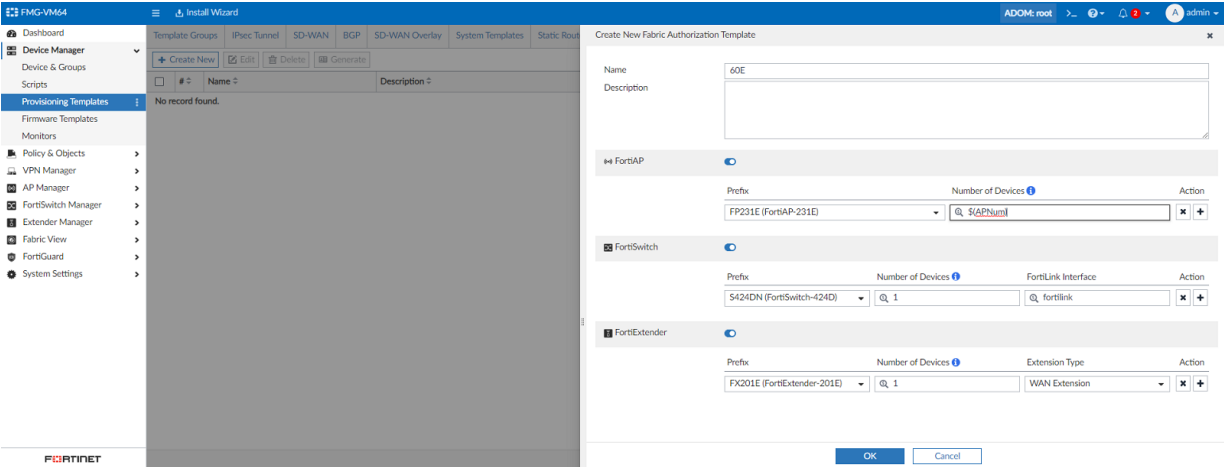
FortiAP	Toggle ON to enable FortiAP in the template.
Prefix	Select a model from the dropdown list, for example <i>FP231E</i> .
Number of Devices	This field determines how many APs will be added, and you can enter a number or use a variable. Entering the \$ sign causes the variable list to appear where you can select a variable from the dropdown list. This example uses the \$ (APNum) variable.

- b. FortiSwitch:

FortiSwitch	Toggle ON to enable FortiSwitch in the template.
Prefix	Select a model from the dropdown list, for example <i>S424DN</i> .
Number of Devices	This field determines how many FortiSwitches will be added, and you can enter a number or use a variable. This example uses the number 1.
FortiLink Interface	Enter the interface name. This field supports variables. This example uses the name <code>fortilink</code> .

c. FortiExtender:

FortiExtender	Toggle ON to enable FortiExtender in the template.
Prefix	Select a model from the dropdown list, for example <i>FX201E</i> .
Number of Devices	This field determines how many FortiExtenders will be added, and you can enter a number or use a variable. This example uses the number 1.
FortiLink Interface	Select an extension type from the dropdown list. This example uses <i>WAN Extension</i> .



4. Click **OK** to save the Fabric Authorization Template.

Step 2: Add a Fabric Authorization Template to a device blueprint

To add the Fabric Authorization Template to a device blueprint:

1. Go to Device Manager. In the *Device & Group* window, click the *Add Device* dropdown and choose *Device Blueprint* to create a new device blueprint.
2. Configure the device blueprint. For example:

Name	Enter a name for the blueprint. In this example, it is <i>60E</i> .
Device Model	Select a device platform, for example <i>FortiGate-60E</i> .
Fabric Authorization Template	Select the previously configured Fabric Authorization Template (<i>60E</i>).

3. Click **OK** to save the device blueprint.

Step 3: Add the device blueprint to a model device

To add the Fabric Authorization Template to a model device:

1. Go to Device Manager. In the *Device & Group* window, click *Add Device > Add Model Device*.
2. Configure the model device using the device blueprint. For example:

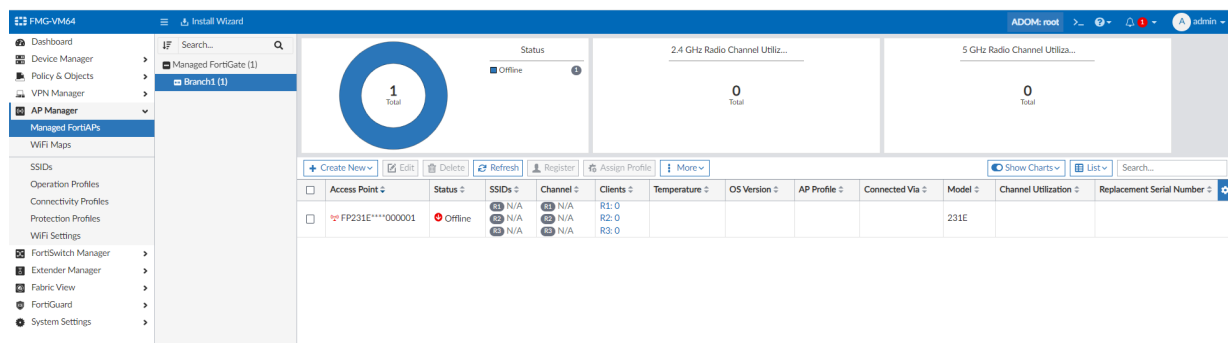
Name	Enter the FortiGate's name. In this example, it is <code>Branch1</code> .
Link Device By	Select <i>Serial Number</i> .
Serial Number	Enter the serial number.
Use Device Blueprint	Enable the <i>Use Device Blueprint</i> setting.
Device Blueprint	Select the previously configured device blueprint (<code>60E</code>)

3. Click **OK** to save the model device.

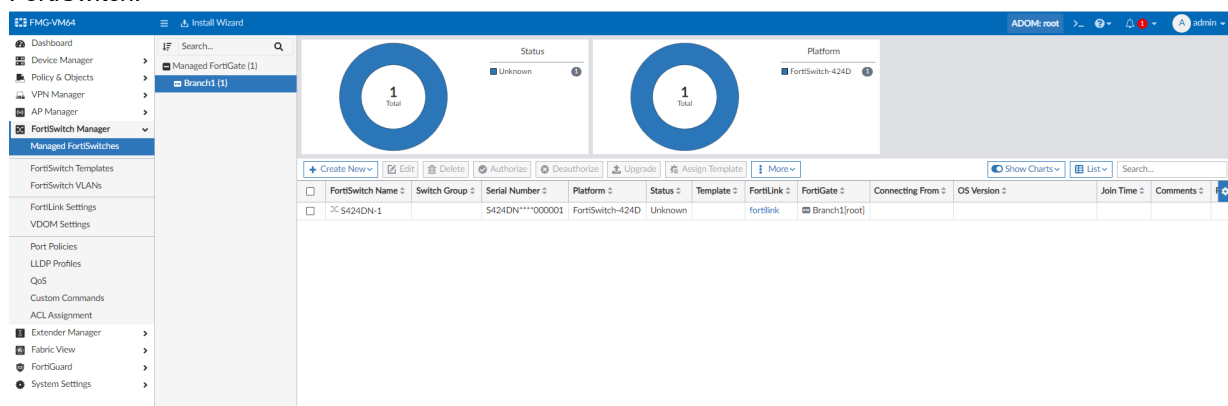
Step 4: View the configured FortiAP, FortiSwitch, and FortiExtender

1. After the device is added to the Device Manager, go to the *AP Manager*, *FortiSwitch Manager*, and *Extender Manager* in FortiManager and you can see that the FortiGate has been automatically configured with a FortiAP, FortiSwitch and FortiExtender as defined by the template.
For example:

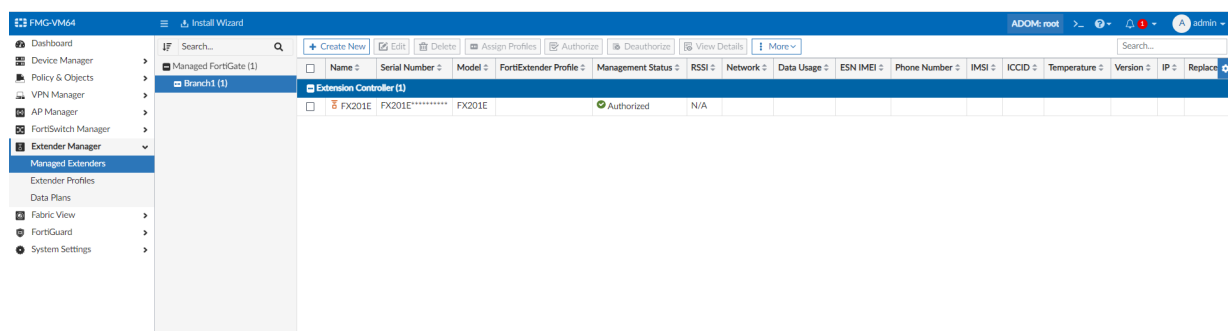
FortiAP:



FortiSwitch:



FortiExtender:



Central Management

This section lists the new features added to FortiManager for central management:

- [AP Manager on page 46](#)
- [FortiSwitch Manager on page 50](#)
- [Others on page 59](#)

AP Manager

This section lists the new features added to FortiManager for AP manager:

- [Multiple optimizations to the factory default SSID and AP-profiles 7.4.1 on page 46](#)

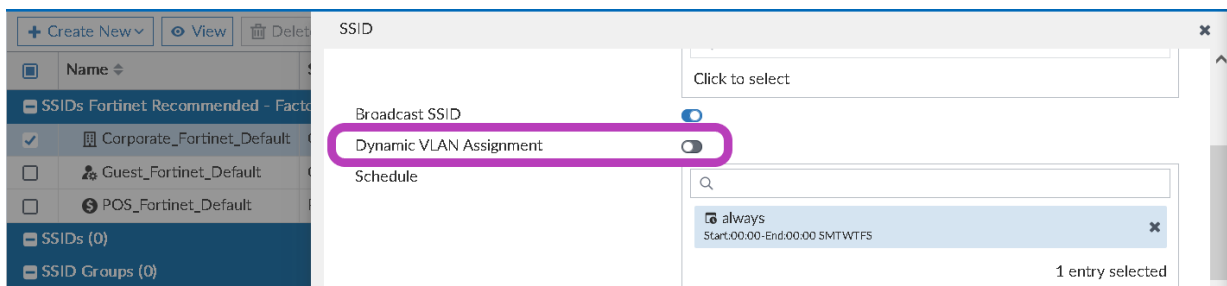
Multiple optimizations to the factory default SSID and AP-profiles - 7.4.1

In FortiManager 7.4.1, there are multiple optimizations to the factory default SSID and AP-profiles.

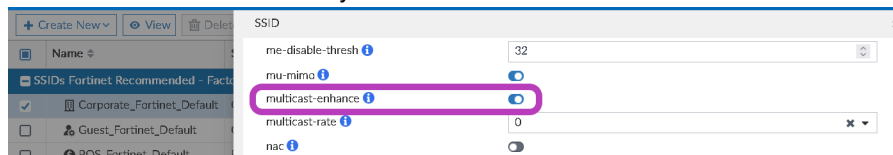
- [Fortinet recommended factory default SSIDs on page 46](#)
- [Fortinet recommended factory default AP Profiles on page 47](#)
- [Fortinet recommended factory default ARRP Profile on page 49](#)

Fortinet recommended factory default SSIDs

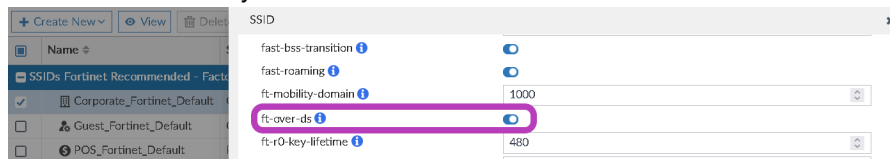
- All three Fortinet recommended factory default SSID templates allow users to select the traffic mode as either Bridged or Tunnel when the templates are activated.
- The *Corporate_Fortinet_Default* SSID includes the following changes:
 - *Dynamic VLAN Assignment* - disabled by default.



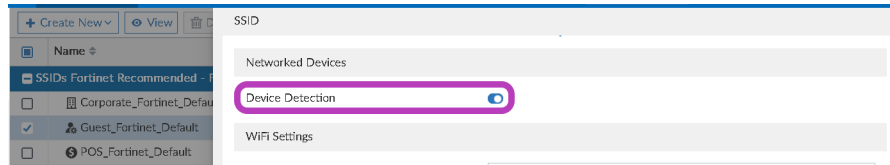
- *multicast-enhance* - enabled by default.



- *ft-over-ds* - enabled by default.



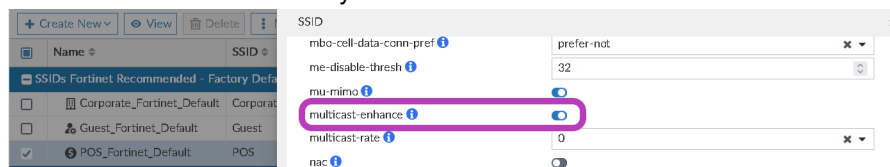
- The *Guest_Fortinet_Default* SSID includes the following changes:
 - *Device Detection* - enabled by default.



- *multicast-enhance* - enabled by default.

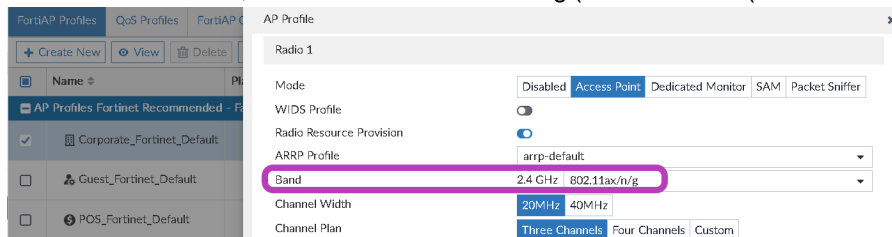


- The *POS_Fortinet_Default* SSID includes the following changes:
 - *multicast-enhance* - enabled by default.

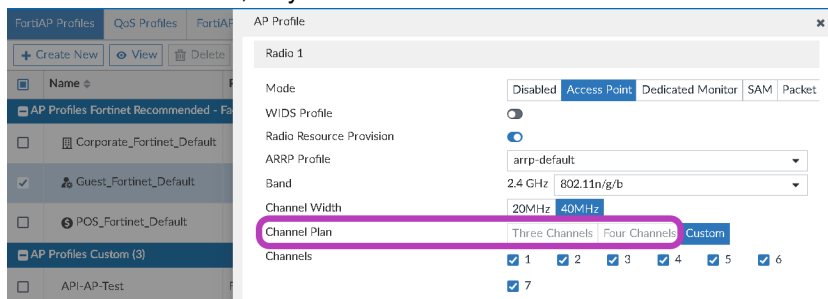


Fortinet recommended factory default AP Profiles

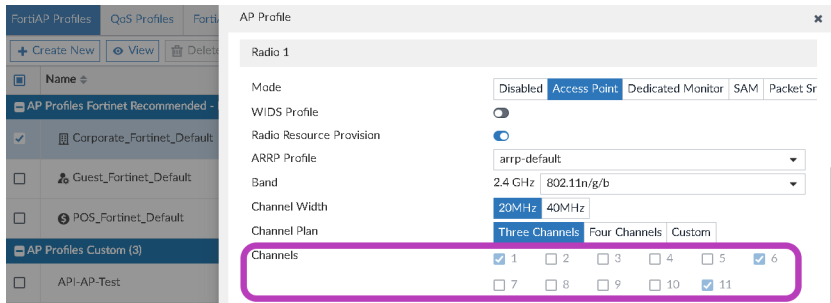
- For the 2.4 GHz band, set the default 802.11 ax/n/g (for WiFi6/6E/6 (Smart Series)).



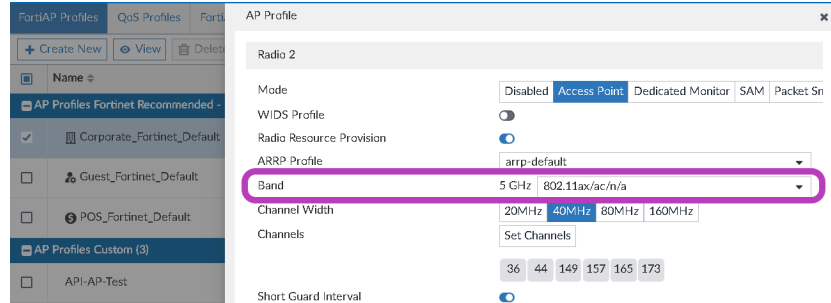
- For the 2.4 GHz band, only allow 20MHz channel width.



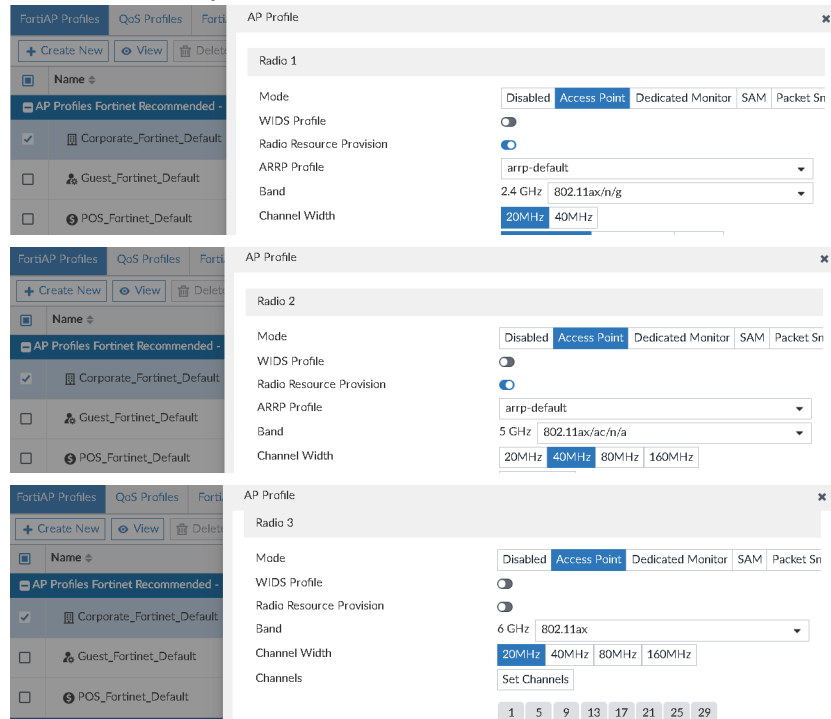
- Enforce the 2.4 GHz radio 1 on *Three Channels* (some profiles are on three channels "custom").



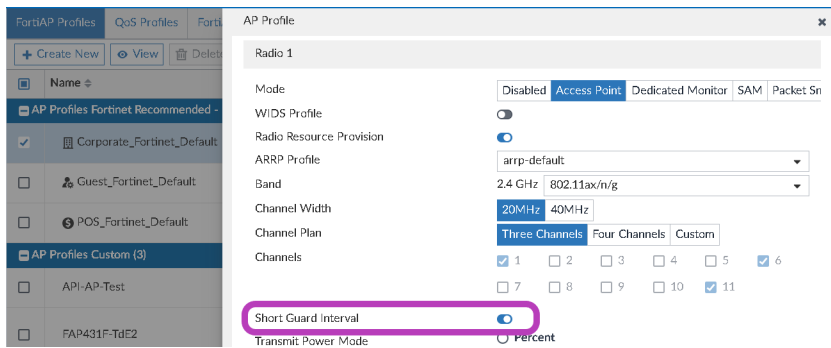
- For the 5 GHz band (radio 2), set to 802.11 ax/ac/n/a (for WiFi6/6E/6 (Smart Series)).



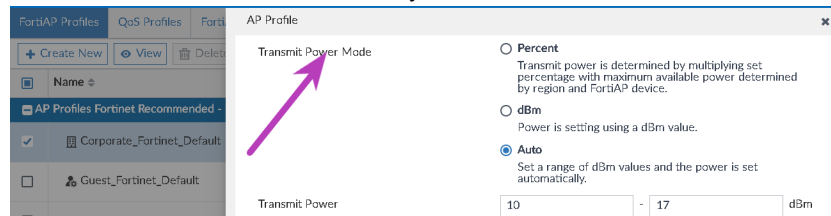
- Enable all radios by default.



- Short Guard Interval* - enabled by default on all radios.

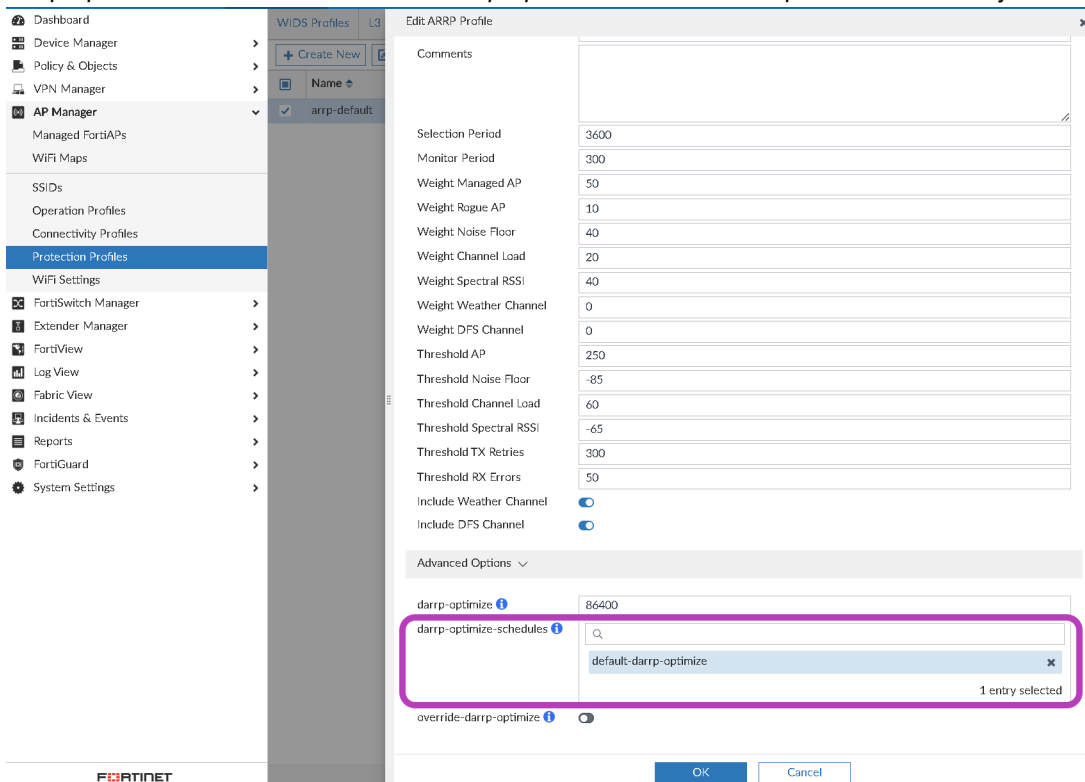


- **Transmit Power Mode** - set to Auto by default on all radios.



Fortinet recommended factory default ARRP Profile

- **darrp-optimize-schedules** - The *default-darrp-optimize* schedule in the profile is selected by default.



FortiSwitch Manager

This section lists the new features added to FortiManager for FortiSwitch manager:

- Per-device VRRP mapping can be used under FortiSwitch Profiles on page 50
- FortiManager allows switchport export to another VDOM, and configuration of the exported port in the destination VDOM on page 51
- FortiSwitch replacement procedure can be executed from FortiManager GUI on page 54
- Custom commands can be assigned/unassigned at once to multiple managed FortiSwitches 7.4.1 on page 56

Per-device VRRP mapping can be used under FortiSwitch Profiles



This information is also available in the FortiManager 7.4 Administration Guide:

- [Creating FortiSwitch VLANs](#)

FortiManager supports per-device mapping for Virtual Router Redundancy Protocol (VRRP) in FortiSwitch profiles.

To configure per-device mappings for VRRP settings in a FortiSwitch profile:

1. Go to *FortiSwitch Manager > FortiSwitch VLANs*.
2. Create or edit a VLAN interface, and make a per-device mapping for a FortiGate.

Edit Per-Device Mapping

Mapped Device: FortiGate-300E
 VLAN ID: 22
 IP/Network Mask: 192.168.122.1/255.255.255.255

Mapped DHCP Server: **OFF** | Server | Relay

VRRP

ID	Group ID	IP	Destination IP	Status
11	11	10.10.11.1	10.10.111.1	Enabled

Restrict Access

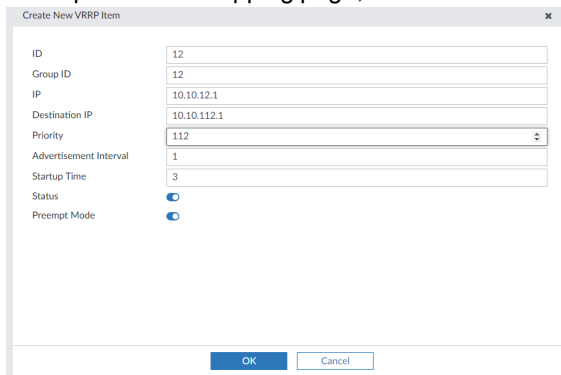
IPv6 Administrative Access: ☐ HTTPS ☐ PING ☐ SSH ☐ SNMP ☐ HTTP ☐ TELNET ☐ FMG-Access ☐ Security Fabric Connection

Secondary IP Address: ☐

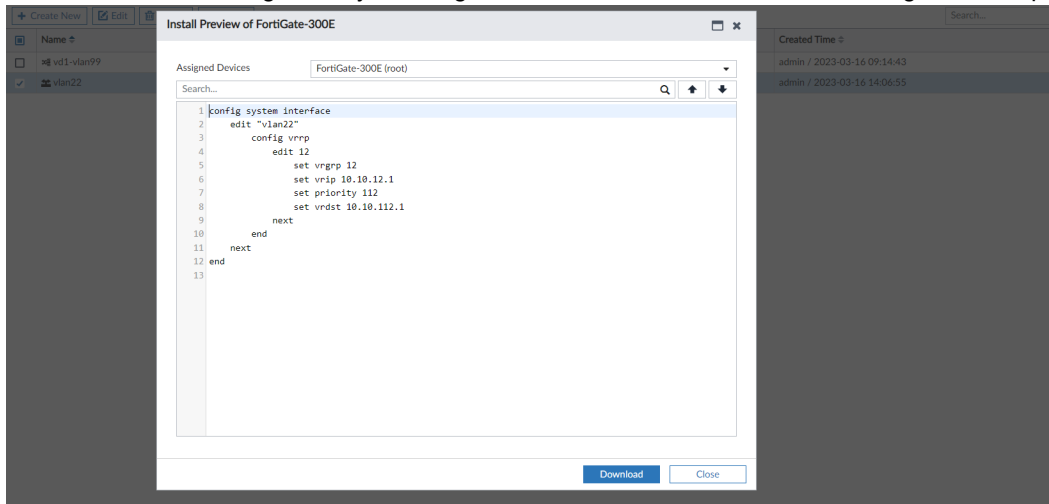
IPv4 Advanced Options >
 IPv6 Advanced Options >

OK **Cancel**

3. In the per-device mapping page, users can add a VRRP setting for the FortiSwitch VLAN.



4. When the VLAN is being used by an assigned FortiSwitch VLAN, the VRRP setting can be deployed.



FortiManager allows switchport export to another VDOM, and configuration of the exported port in the destination VDOM



This information is also available in the FortiManager 7.4 Administration Guide:

- [Exporting FortiSwitch ports to another VDOM](#)

FortiManager allows switchport export to another VDOM, and configuration of the exported port in the destination VDOM.

To export FortiSwitch ports:

1. Disable *FortiSwitch Central Management* in *System Settings > All ADOMs*.

The screenshot shows the FortiManager Central Management interface. On the left, a list of ADOMs is displayed, with '720' selected. On the right, the 'Edit ADOM' window is open for ADOM 720. The 'Central Management' section is expanded, and the 'FortiSwitch' checkbox is checked and highlighted with a red box. Other settings like 'Normal', 'Backup', 'VPN', 'FortiAP', and 'FortiSwitch' are visible. The 'Status' is set to 'On'.

2. Add a Multi-VDOM enabled FortiGate with an attached FortiSwitch.

The screenshot shows the FortiManager FortiSwitch Manager interface. On the left, a list of managed FortiGates is shown, with 'root' selected. On the right, the 'Ports Configuration' window is open for FortiSwitch S248DF3X17000116. The 'port12' is highlighted. The table below shows the configuration for each port.

Port	Description	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	POE	Device Information	DHCP Snooping	Transceiver
port1		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port2		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port3		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port4		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port5		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port6		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port7		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port8		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port9		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port10		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port11		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port12		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port13		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port14		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port15		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port16		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port17		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	
port18		Static		Edge Port, Spanning Tree Protocol	_default	quarantine	Powered		Untrusted	

3. Go to *FortiSwitch Manager > Managed FortiSwitches*, right-click on a FortiSwitch and select *Ports Configuration*.

4. Edit a port to enter the *Edit VLAN Assignment* pane, and choose the new VDOM in the *Export To* field.

The screenshot shows the 'Edit VLAN Assignment' configuration pane for port12. The 'Export To' field is highlighted with a red box, showing a dropdown menu with 'root' selected and 'vd1' as an option. Other configuration fields include Port Name (port12), Description, Access Mode (Static), Native VLAN (_default), Allowed VLANs (quarantine), Security Policy (Click to select), LLDP Profile (default-auto-isl), QoS Policy (default), PoE Status (on), DHCP Snooping (off), Loop Guard (off), STP (on), Edge Port (on), STP BPDU Guard (off), STP Root Guard (off), and Advanced Options.

5. After the port is exported, users can edit the port's configuration in the chosen VDOM.

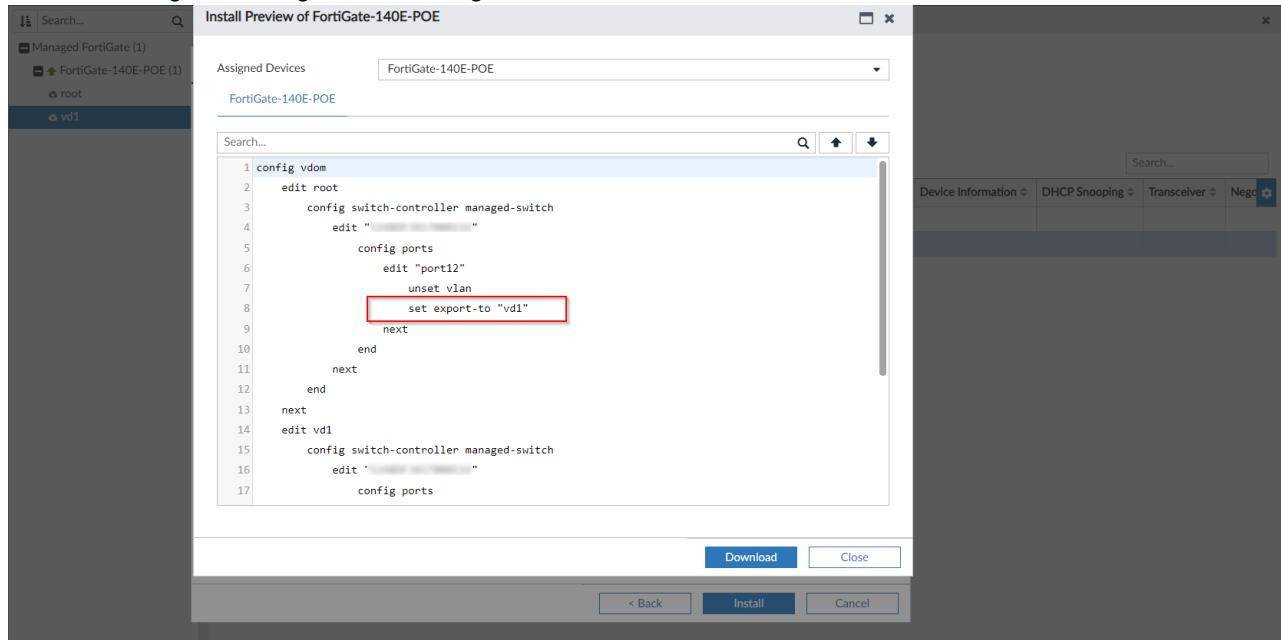
The screenshot shows the 'FortiSwitch Ports' table for S248DF3X17000116. The table has columns: Port, Description, Mode, Port Policy, Enabled Features, Native VLAN, Allowed VLANs, POE, Device Information, DHCP Snooping, Transceiver, and Negotiation. Port12 is highlighted, showing it is assigned to vdom1-vlan99.

Port	Description	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	POE	Device Information	DHCP Snooping	Transceiver	Negotiation
port11					vlan20	All	Powered				
port12					vdom1-vlan99		Powered				

The screenshot shows the 'Edit VLAN Assignment' configuration pane for port12 in the 'vd1' VDOM. The 'Native VLAN' is set to vdom1-vlan99. Other configuration fields include Port Name (port12), Description, Allowed VLANs (vdom1-vlan99), Security Policy (Click to select), LLDP Profile (default), QoS Policy (default), PoE Status (on), and Advanced Options.

The screenshot shows the 'Edit VLAN Assignment' configuration pane for port12 in the 'vd1' VDOM. The 'Native VLAN' is set to vlan20. Other configuration fields include Port Name (port12), Description, Allowed VLANs (All), Security Policy (Click to select), LLDP Profile (default), QoS Policy (default), PoE Status (on), and Advanced Options.

6. After the settings are configured, the changes can be installed to the FortiGate.



FortiSwitch replacement procedure can be executed from FortiManager GUI

FortiSwitch replacement procedure can be executed from the FortiManager GUI.

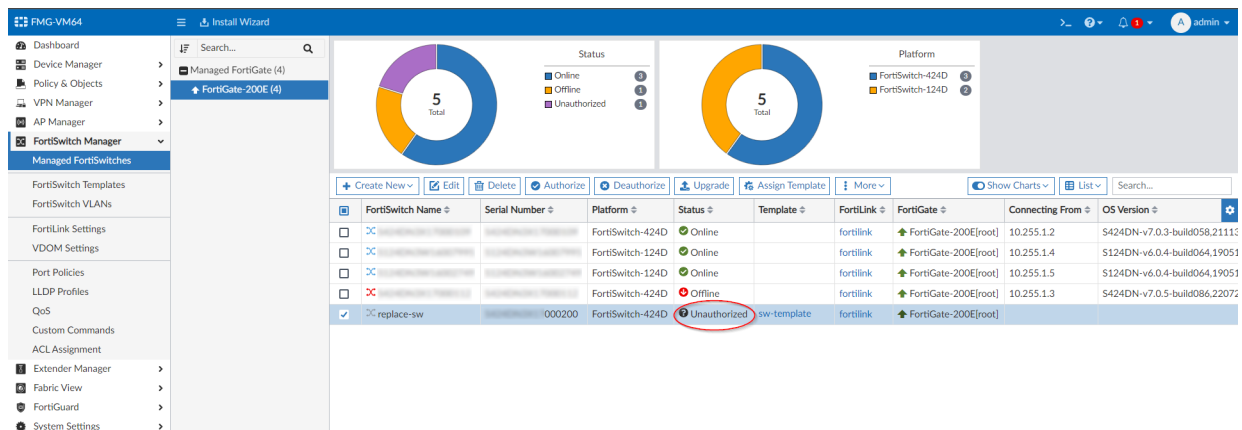


This information is also available in the FortiManager 7.4 Administration Guide:

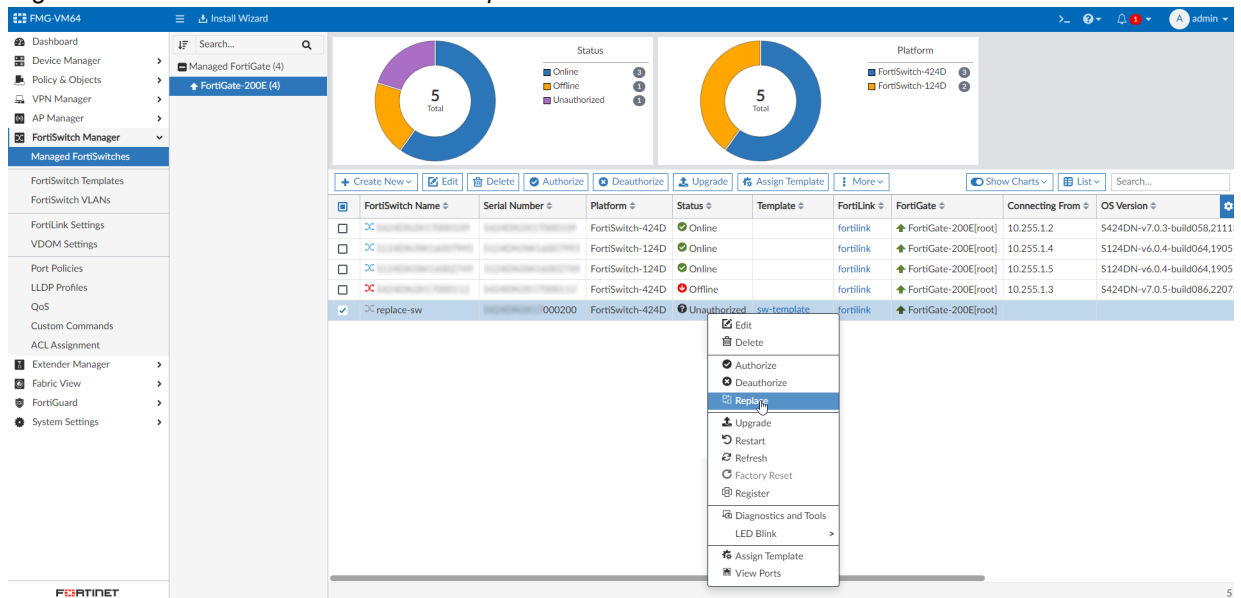
- [Replacing Switches](#)

To replace a FortiSwitch device from the FortiManager GUI:

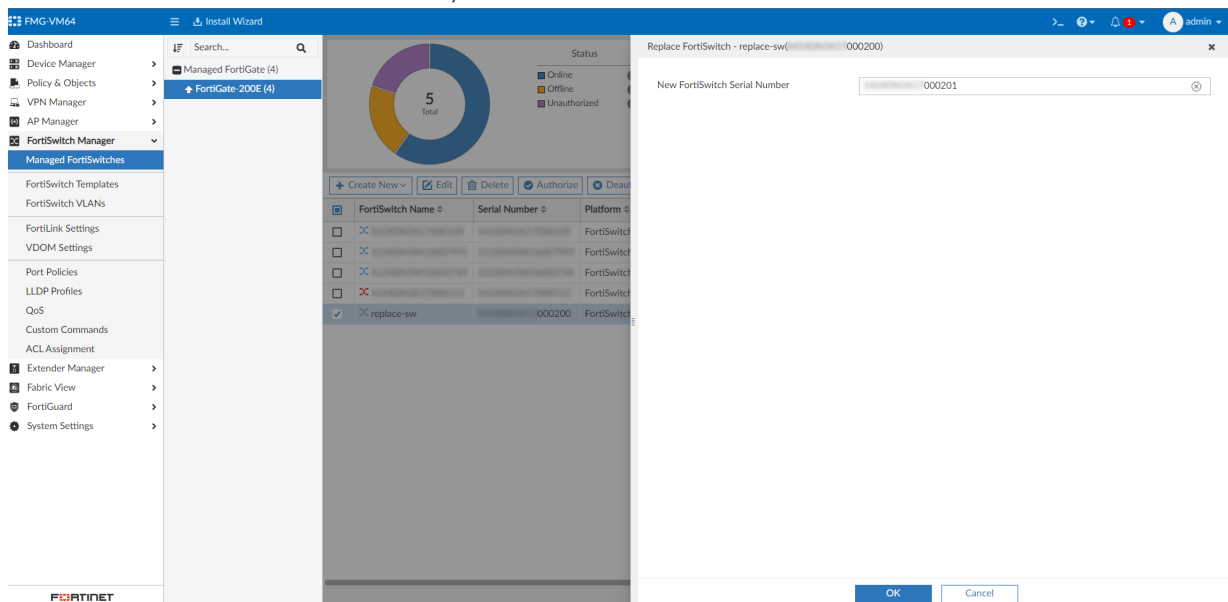
1. Go to *FortiSwitch Manager > Managed FortiSwitches*.
2. Deauthorize the FortiSwitch that will be replaced, and refresh the FortiSwitch list. The FortiSwitch will display with the status *Unauthorized*.



3. Right-click on the FortiSwitch and select *Replace*.



4. Enter the new FortiSwitch serial number, and click *OK* to confirm.



After the operation is complete, refresh the FortiSwitch list. The new FortiSwitch serial number will be displayed,

and the original switch template is kept.

The screenshot shows the FortiManager FMG-VM64 interface. On the left is a navigation menu with options like Dashboard, Device Manager, Policy & Objects, VPN Manager, AP Manager, FortiSwitch Manager, and Managed FortiSwitches. The main area displays the 'Managed FortiSwitches' list. A table lists devices with columns: FortiSwitch Name, Serial Number, Platform, Status, Template, FortiLink, FortiGate, Connecting From, and OS Version. One device, FortiSwitch-424D with serial 000201, is highlighted with a red box and has its status set to 'Unauthorized' and template set to 'sw-template'. Above the table are two donut charts: 'Status' (5 total, 4 Online, 1 Unauthorized) and 'Platform' (5 total, 4 FortiSwitch-424D, 1 FortiSwitch-124D).

5. Authorize the FortiSwitch, and the replacement is complete.

The screenshot shows the FortiManager FMG-VM64 interface after authorization. The 'Managed FortiSwitches' list now shows the FortiSwitch-424D with serial 000201 as 'Online' and with the 'sw-template' assigned. The 'Status' donut chart now shows 5 total devices, all Online. The 'Platform' donut chart remains the same (5 total, 4 FortiSwitch-424D, 1 FortiSwitch-124D).

Custom commands can be assigned/unassigned at once to multiple managed FortiSwitches - 7.4.1



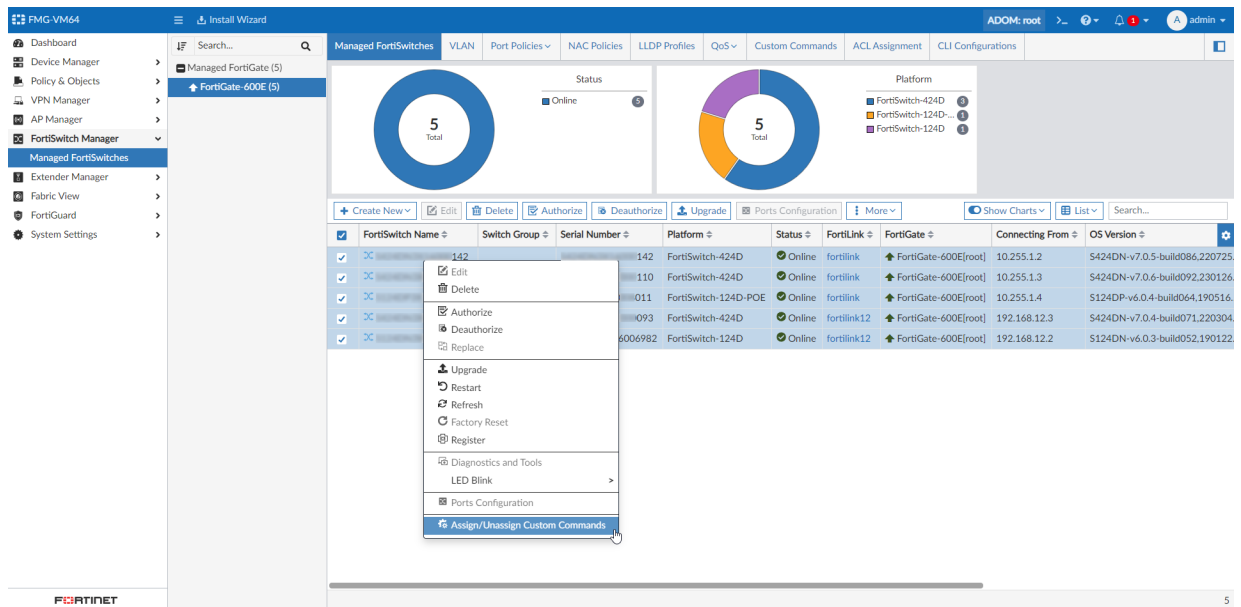
This information is also available in the FortiManager 7.4 Administration Guide:

- [Creating custom commands](#)

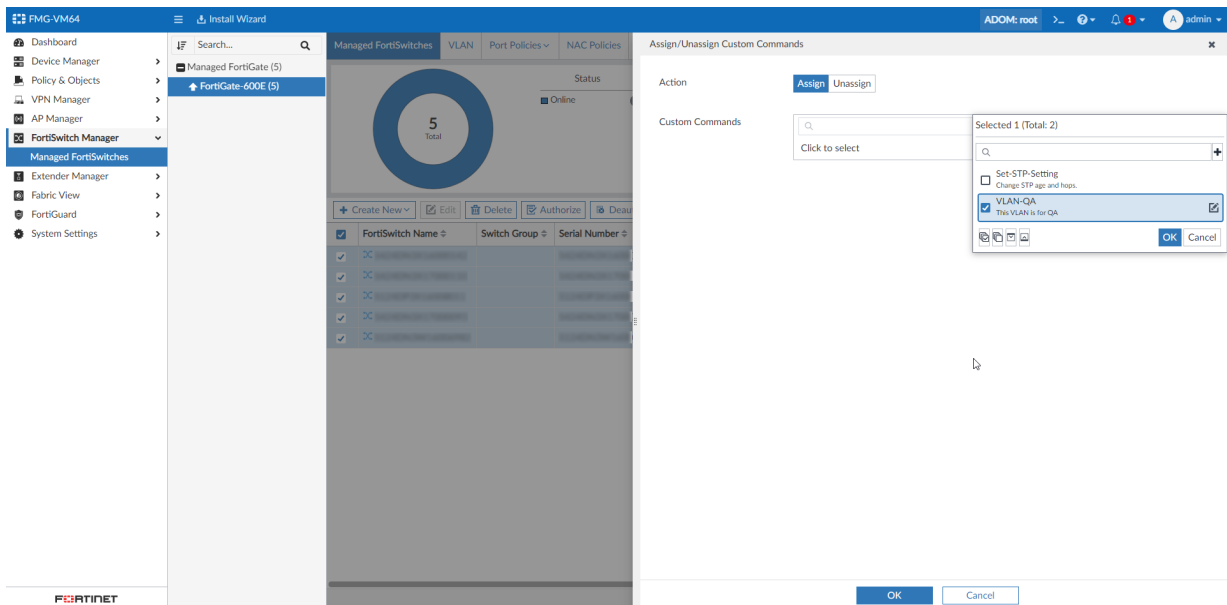
Custom commands can be assigned/unassigned at once to multiple managed FortiSwitches.

To push custom commands to multiple FortiSwitch devices:

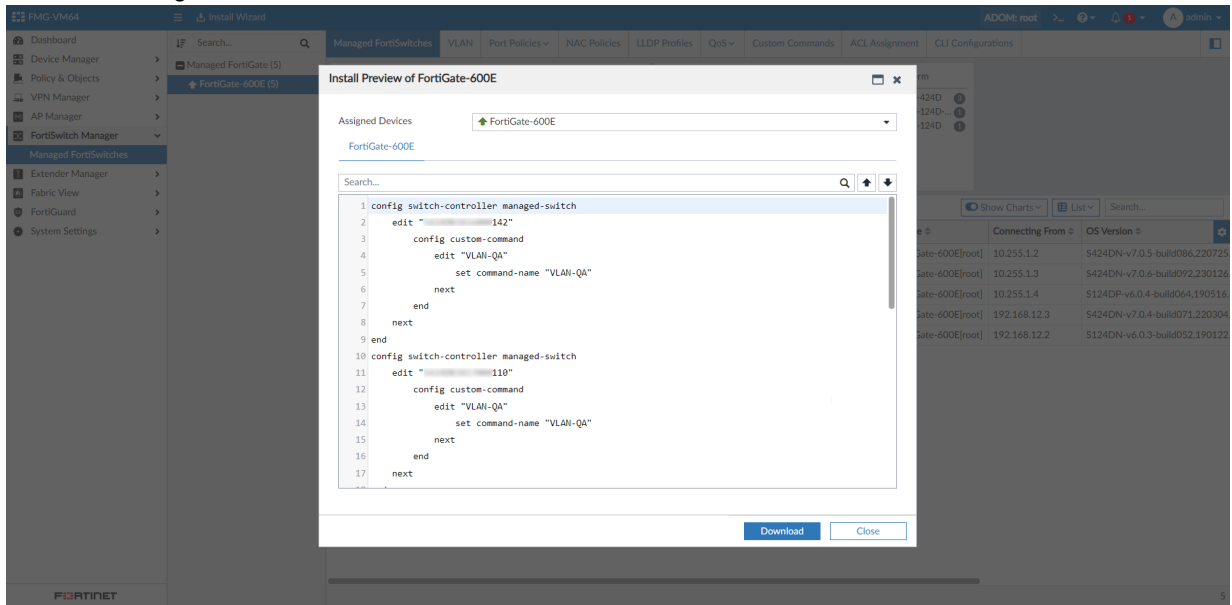
1. In Per-Device FortiSwitch management mode, select the FortiSwitch devices to which you want to assign custom commands. Multiple FortiSwitch devices can be selected at once.



2. Right-click in the table and select *Assign/Unassign Custom Commands* from the context menu. The *Assign/Unassign Custom Commands* dialog appears.
3. Assign custom commands:
 - a. Select the *Assign* tab and choose the custom command from the dropdown list.
 - b. Click *OK*.

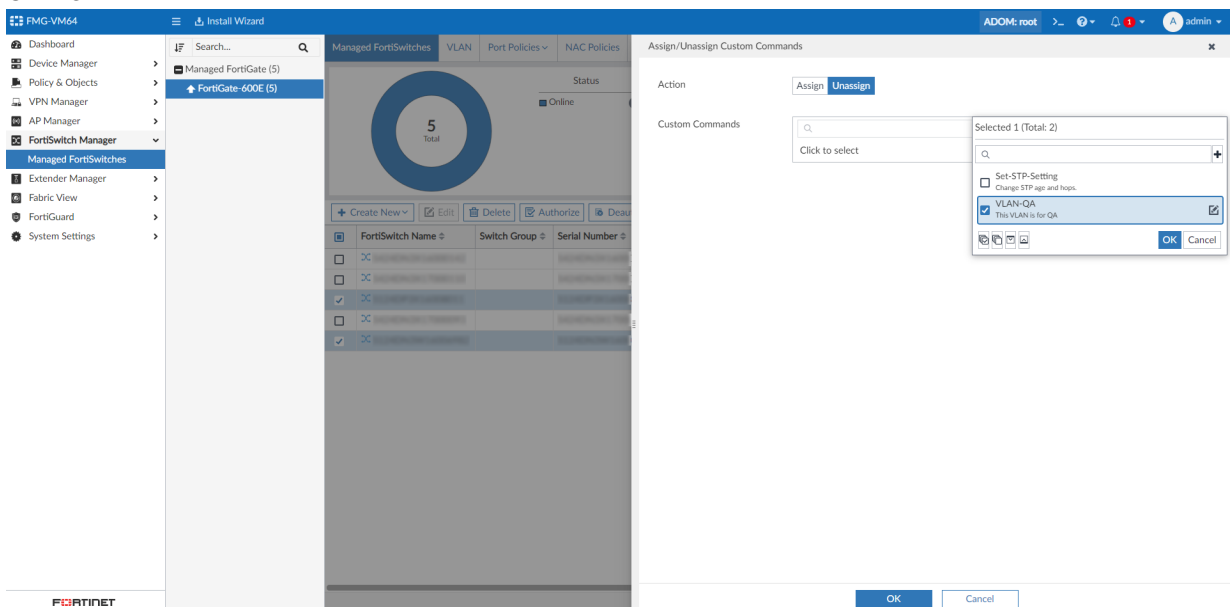


c. Install the changes to the FortiGate devices.

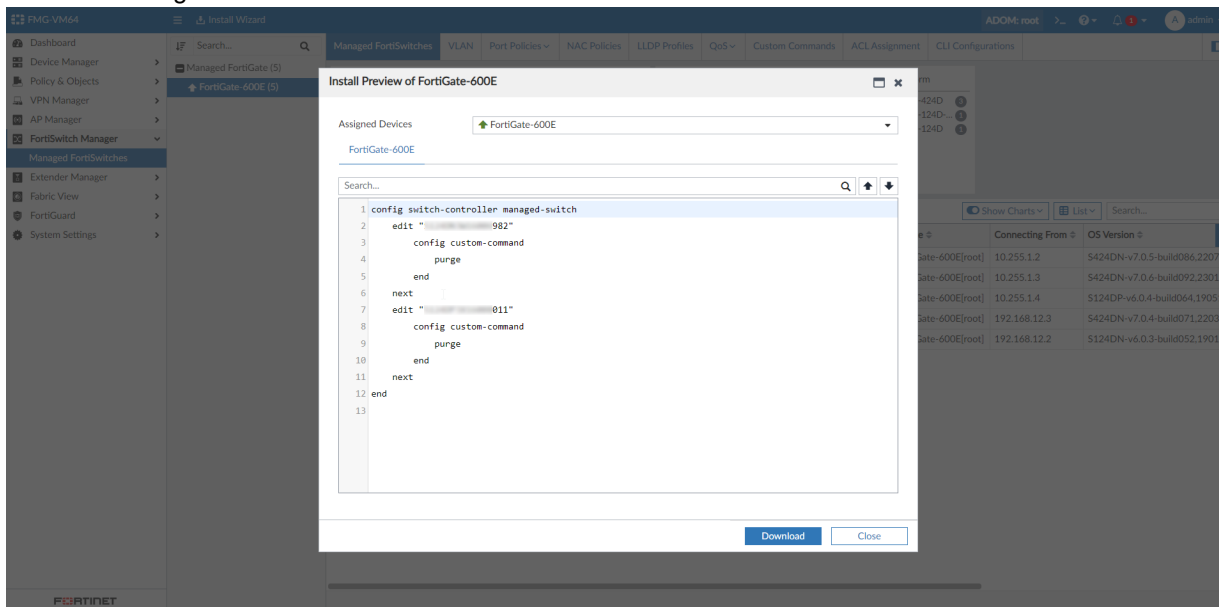


4. Unassign custom commands:

- Select the *Unassign* tab and choose the custom command from the dropdown list.
- Click OK.



c. Install the changes to the FortiGate devices.



Others

This section lists the new features added to FortiManager for other topics relating to central management:

- FortiManager supports install preview for model devices on page 59
- VPN Monitoring displays IPsec VPN tunnels created by IPsec templates and SD-WAN overlay wizard on page 64
- FortiManager supports CLI diff in the workflow approval sessions on page 67

FortiManager supports install preview for model devices



This information is also available in the FortiManager 7.4 Administration Guide:

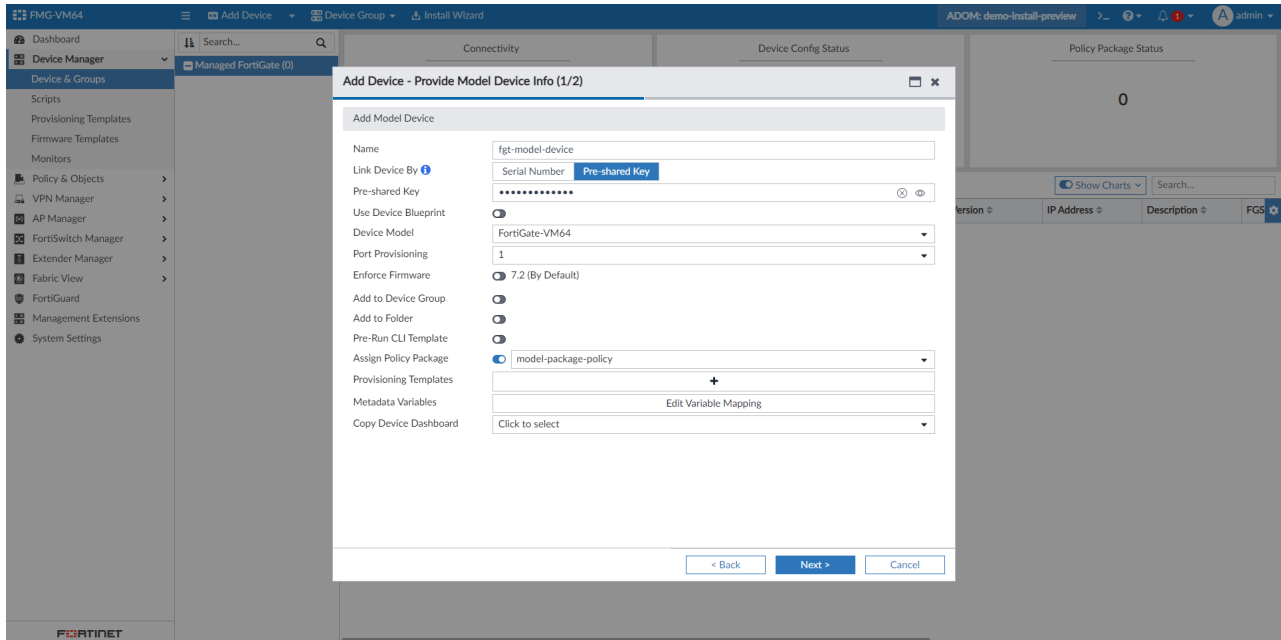
- [Installing policy packages and device settings](#)

Use the *Install Preview* feature in the *Install Wizard* to preview the configuration that will be applied to a model device.

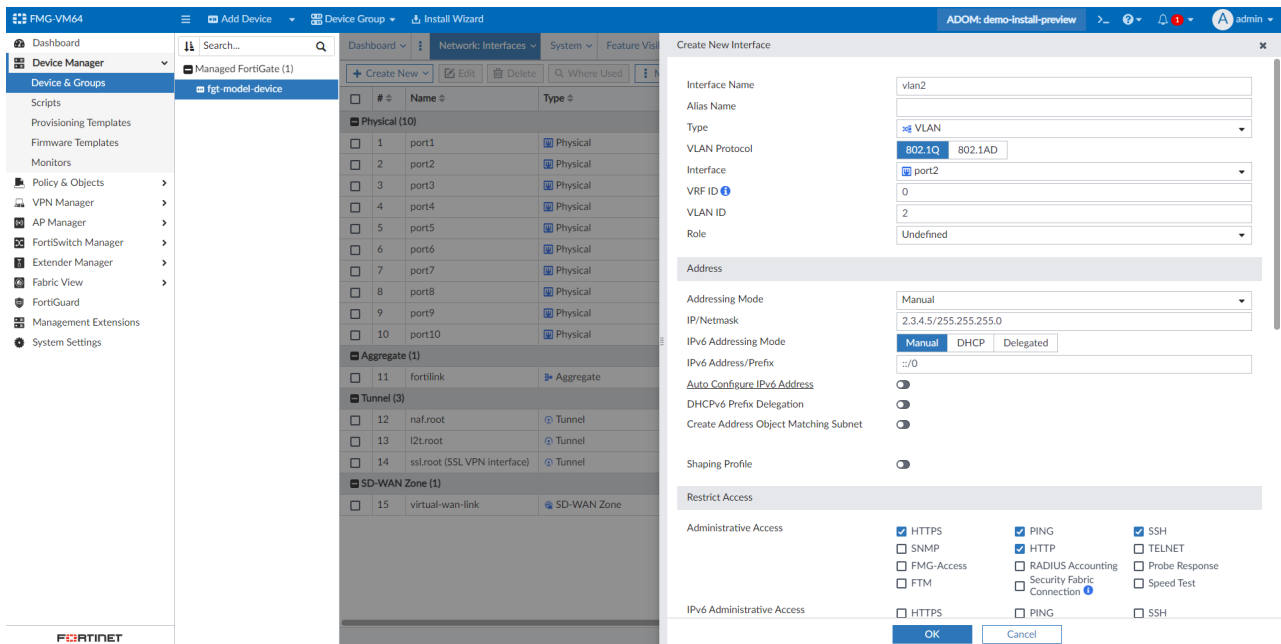
You can make changes to a model device in *Device Manager* or to a policy package that is applied to a model device in *Policy and Objects*. These changes will be saved to the local database of the model device in FortiManager. To preview the actual changes that will be applied, *Install Preview* can be accessed from the *Install Wizard*.

To use *Install Preview* for a model device:

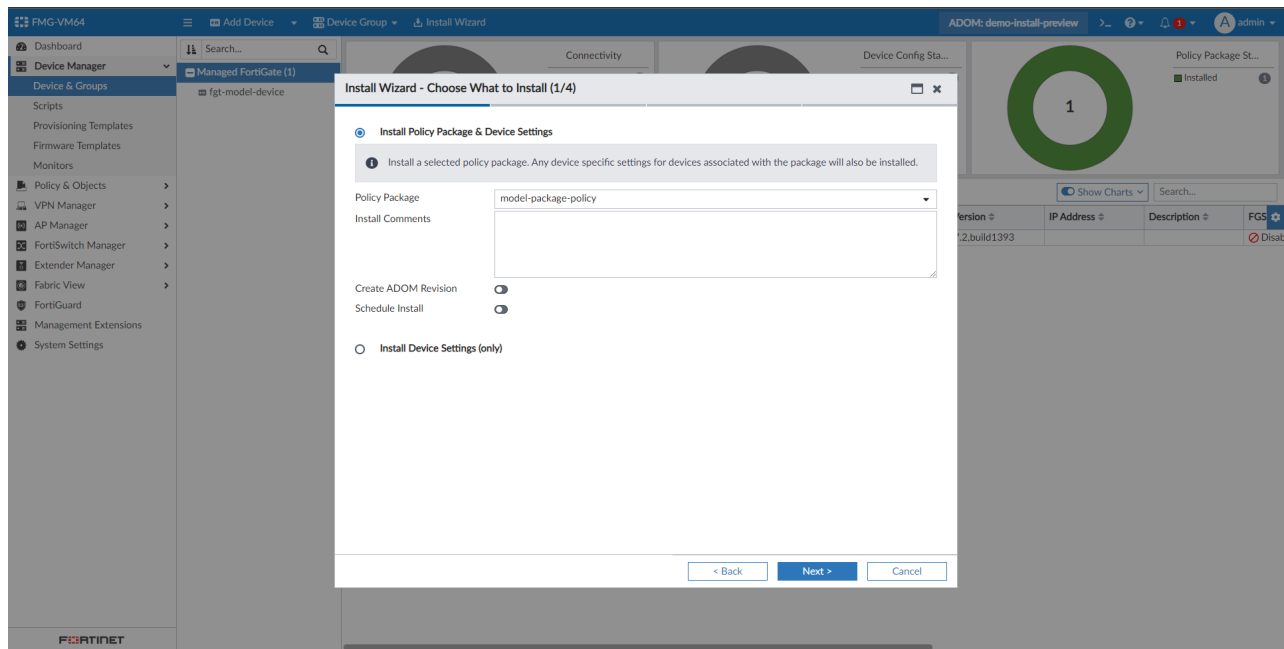
1. Add a model device through *Add Device > Add Model Device*. Assign a policy package.



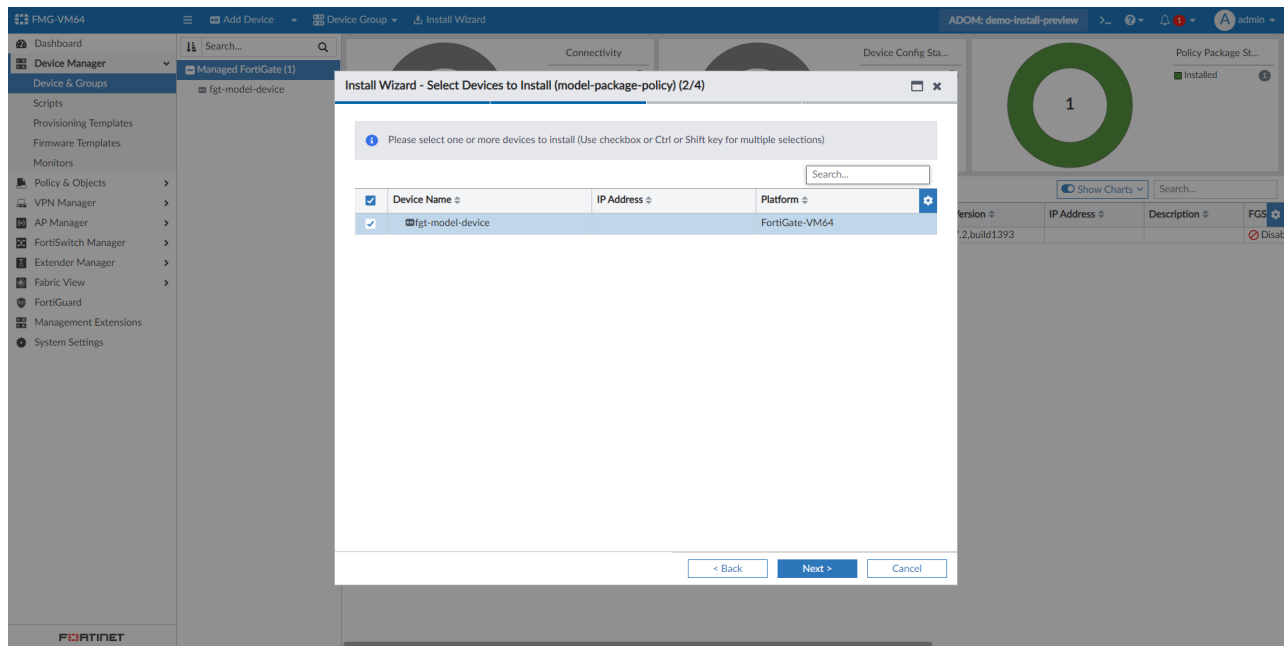
2. Make changes in *Device Manager*. In this example, create a VLAN interface.



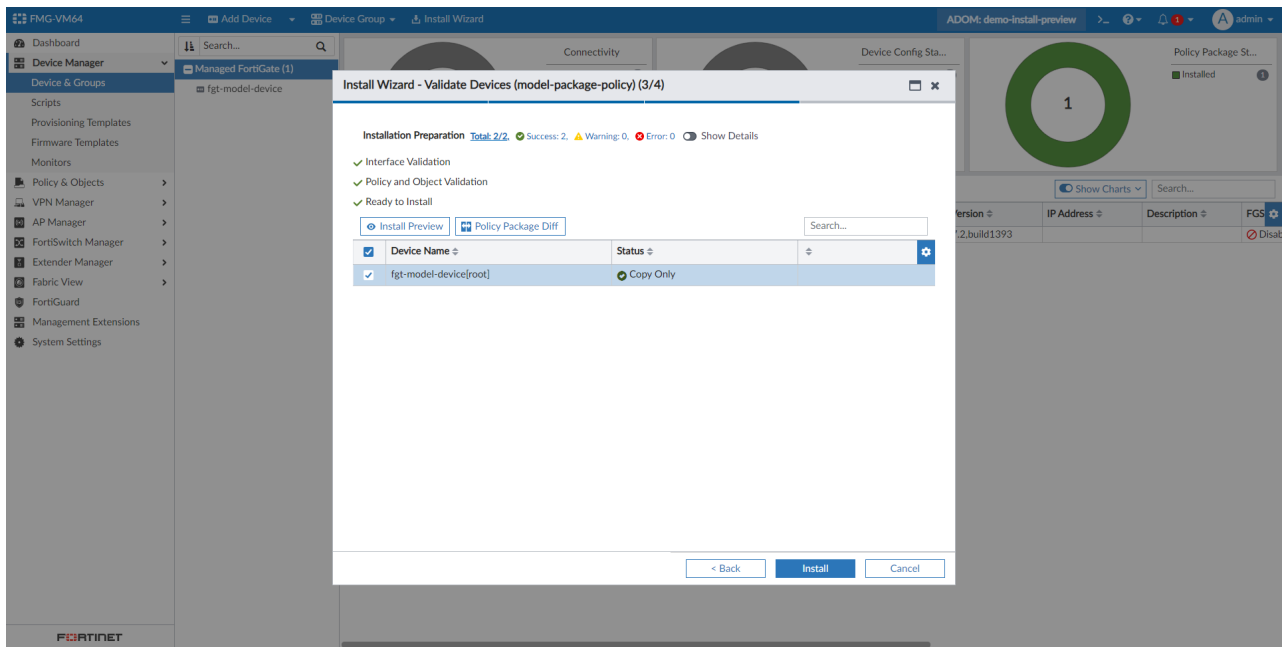
3. Launch *Install Wizard*. Select *Install Policy Package & Device Settings*. Choose the *Policy Package* and click *Next*.



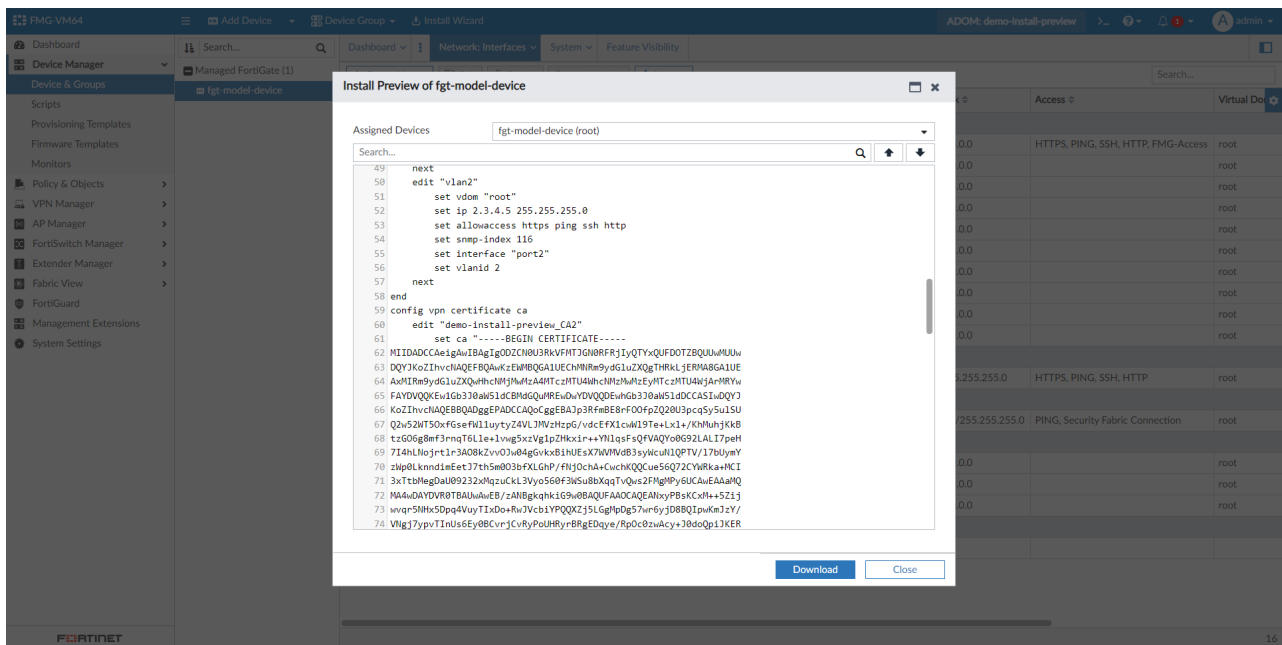
4. Select the target model device and click **Next**.



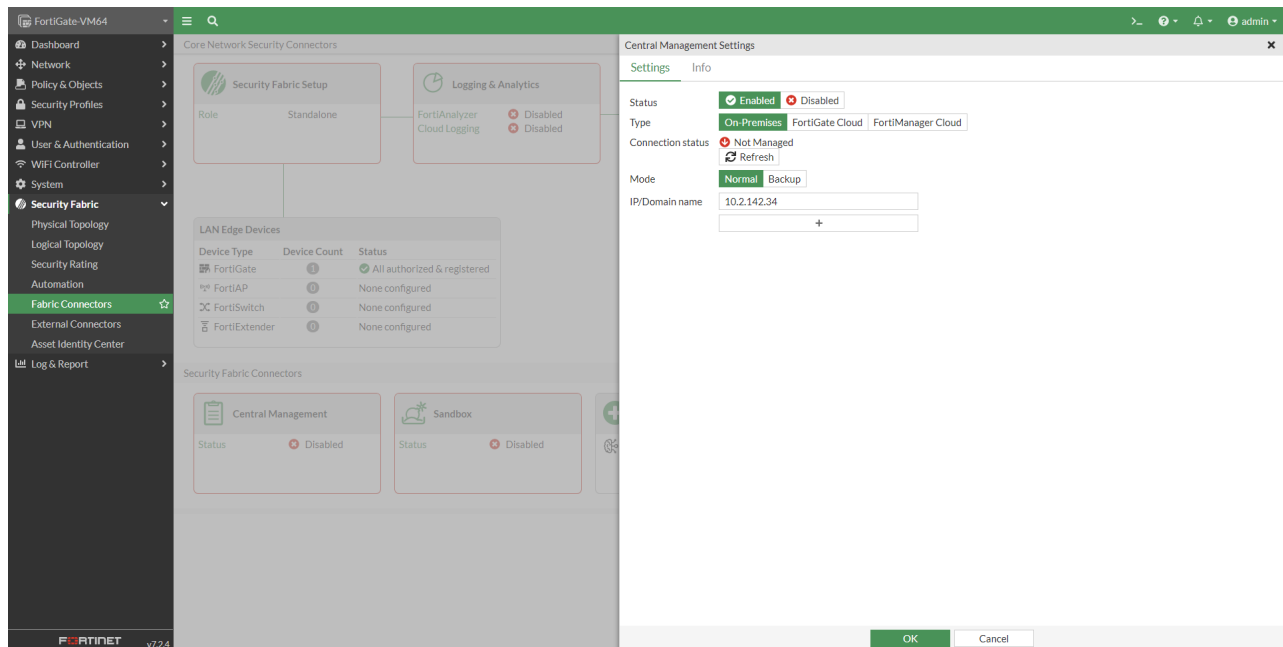
5. Click **Install Preview**.



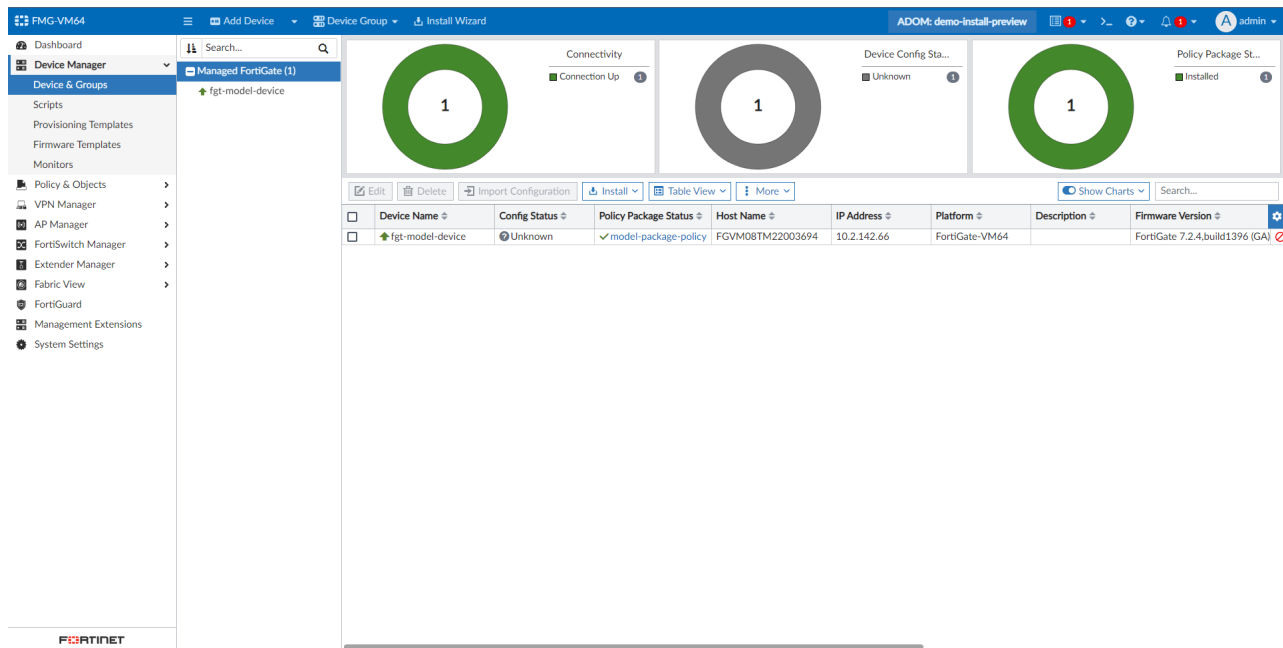
6. In the configuration that is displayed, scroll down to view the new configuration in the system interface table. Use this preview to verify that the new interface is created and is being installed to the model device correctly.



7. Connect the FortiGate to FortiManager to initiate autolink and push the configuration changes.



8. Verify that the device status is changed to *Online*.



9. From *Task Monitor*, view the install log to verify the change is being pushed to the device successfully.

The screenshot displays the FortiManager 7.4.0 Central Management interface. The left sidebar shows the navigation menu with options like Dashboard, Device Manager, Policy & Objects, VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, Fabric View, FortiGuard, Management Extensions, and System Settings. The main panel is titled 'Task Monitor' and shows a list of tasks with columns for ID, Source, Description, User, and Status. A 'View Install Log' window is open on the right, showing the output of an installation process for ADOM: demo-install-preview. The log includes commands like 'config system interface', 'edit "vlan2"', 'set vdom "root"', 'set ip 2.3.4.5 255.255.255.0', 'set allowaccess https ping ssh http', 'set snmp-index 116', 'set interface "port2"', 'set vlanid 2', 'next', and 'end'. The log concludes with 'install finished'.



Some configurations that originally exist in a real device could significantly impact the accuracy of the install preview during an autolink operation.

Examples of these configurations include:

- Hardware specifications.
- Firmware versions and builds.
- Overlapping configurations.

VPN Monitoring displays IPsec VPN tunnels created by IPsec templates and SD-WAN overlay wizard



This information is also available in the FortiManager 7.4 Administration Guide:

- [VPN Monitor](#)

VPN Monitoring displays IPSec VPN tunnels created by IPsec Templates and the SD-WAN Overlay Wizard with specific device icon identification for HUBs and the ability to drilldown to a device group level.

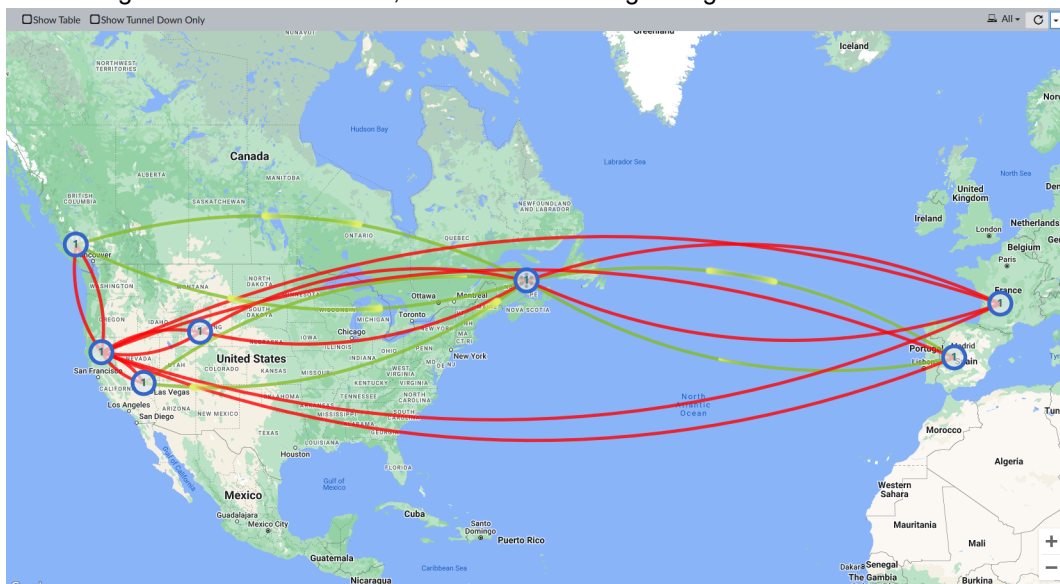
To view IPsec tunnel template information in the VPN Monitor:

1. Go to *Device Manager > Monitors > VPN Monitor*.

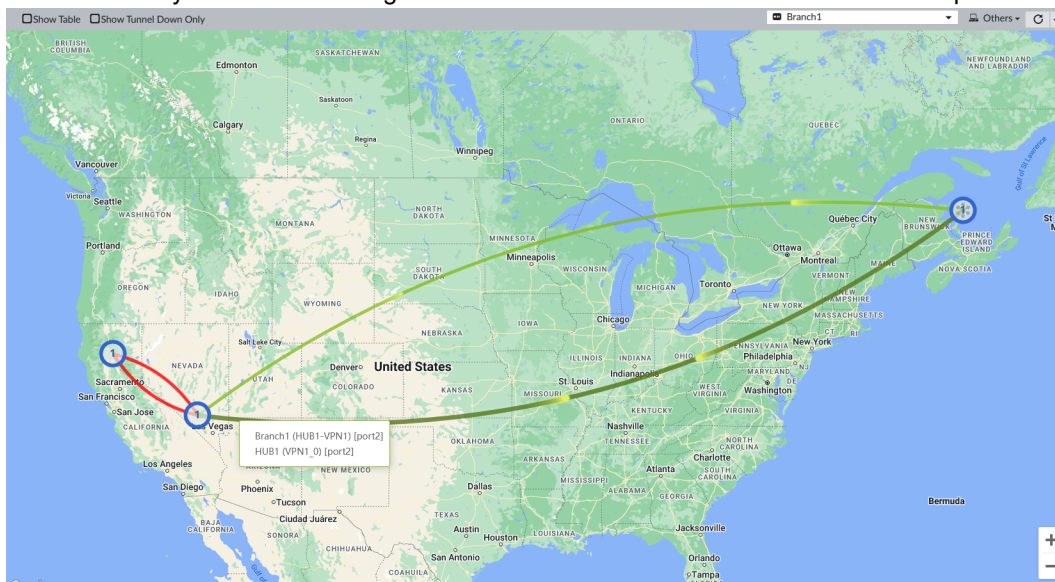
The VPN Monitor displays all IPsec VPN tunnel information created with the VPN Manager, IPsec template, or created directly on FortiOS.

2. The map includes the following information:

- Green lines indicate that a tunnel is up.
- When the green lines are animated, there is traffic flowing through the VPN tunnels.

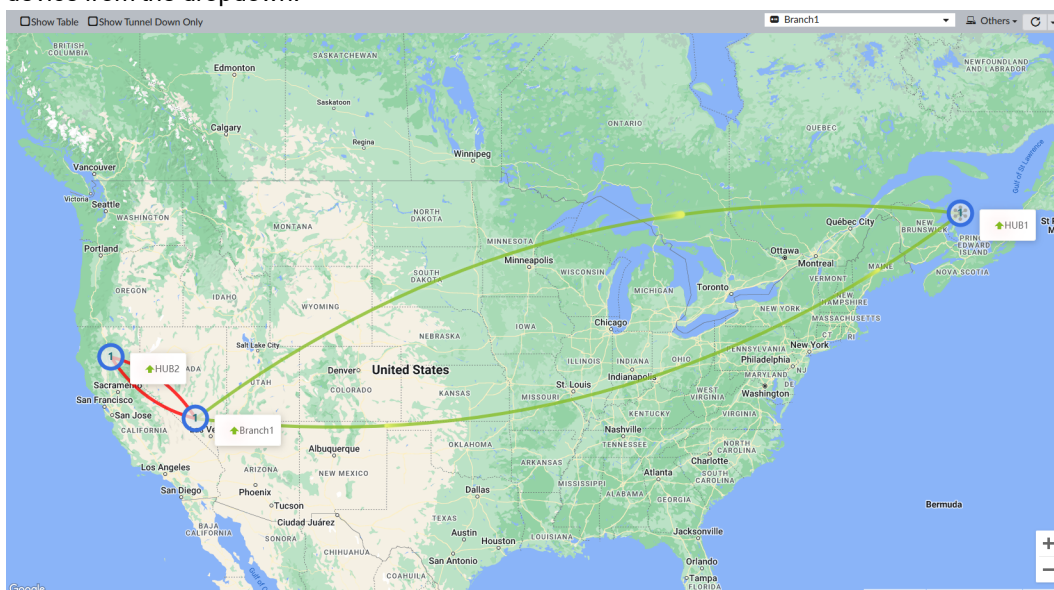


- You can hover your mouse over a green line to view the VPN tunnel name and source port information.

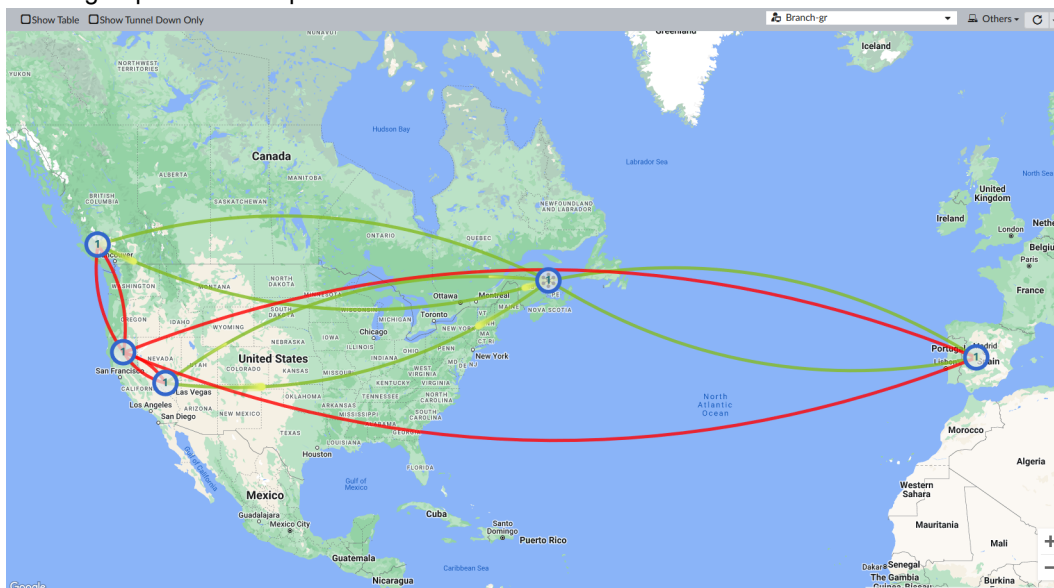


- Red lines indicate that a tunnel is down.
- HUB device(s) are identified with a star icon.

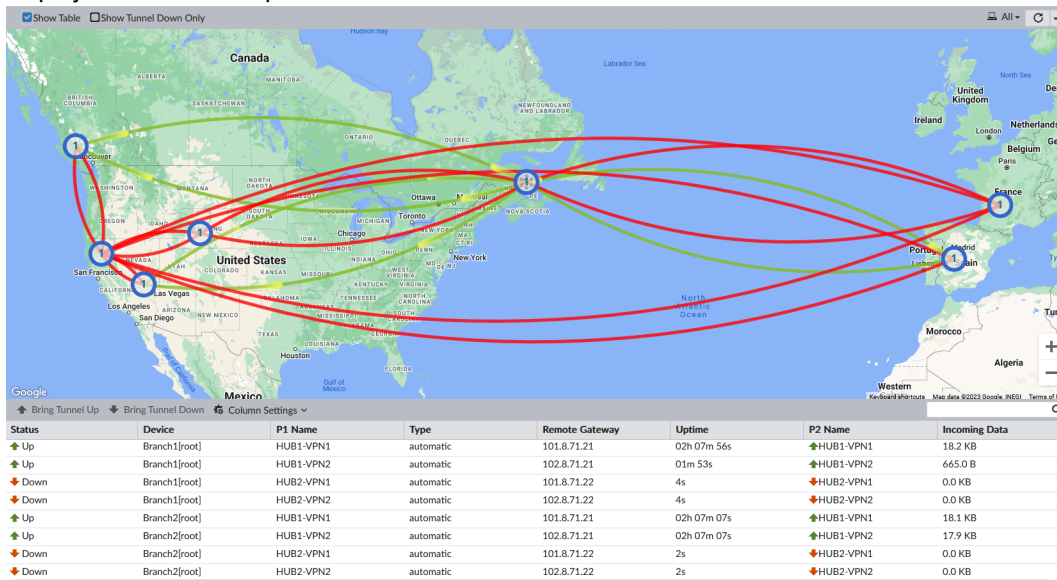
3. To view a single device's IPsec VPN tunnel information, change *All* to *Others* in the toolbar menu, and select a device from the dropdown.



4. To view a device group's IPsec VPN tunnel information, change *All* to *Others* in the toolbar menu, and select a device group from the dropdown.



5. To view IPsec VPN tunnel information in a table, select the *Show Table* option from the toolbar and the table will be displayed under the map.



FortiManager supports CLI diff in the workflow approval sessions



This information is also available in the FortiManager 7.4 Administration Guide:

- [View session diff](#)

FortiManager supports CLI diff in the workflow approval sessions.

To view the CLI diff in workflow approvals:

1. In *Workflow* mode, create a session and make some changes.
2. Save the changes, and click *View Diff*.
The Revision Diffs dialog includes the new *CLI Diff* option.

Revision Diffs Between 1 and 2

Summary

Global Policy -

Have no difference on global policy package.

Policy Package - changed (1)

Policy Package	Install On	User	Update Time	Change Summary
default		admin	2023-04-21 13:43:04	changed [Details] [CLI Diff]

ADOM Level Object - added (2) [\[Details\]](#) [\[CLI Diff\]](#)

Category	User	Update Time	Change Summary
firewall address	admin	2023-04-21 13:43:57	added (1)
webfilter profile	admin	2023-04-21 13:44:42	added (1)

Download

Close

- Click **View Details** to see details of the change and if entries are new changes or modifying existing changes.

Revision Diffs Between 1 and 2

Summary

default ✕

firewall policy - added (1) changed (1)

	#	Policy ID	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Log	Status	Security Profiles	Policy Section	Install On	Others
Changed	1	1	test-1-change test-1	"port1" "any"	"port18" "any"	"all"	"all"	"always"	"ALL"		✓	✓	✓	"default", "default", "default", "no-inspection" "default", "no-inspection"			uuid: d3dab308- e084-51ed- 061b- f386bf1a9bf
Added	3	3	add-policy	"any"	"any"	"all"	"all"	"always"	"ALL"		✓	✓	✓	"default", "default", "no-inspection"			uuid: 1d070c48- e085-51ed- 401f- 6e7e9c74d4

Download

Close

- Click **CLI Diff** to see more specific configuration changes in the CLI.

Revision Diffs Between 1 and 2

CLI Diff

Search...

```

1 config firewall policy
2 edit 1
3 set srcintf "port1"
4 set dstintf "port18"
5 set utm-status enable
6 set av-profile "default"
7 set webfilter-profile "default"
8 set name "test-1-change"
9 next
10 edit 3
11 set name "add-policy"
12 set uuid 1d070c48-e085-51ed-401f-6e7e9c74d4e0
13 set action accept
14 set srcintf "any"
15 set dstintf "any"
16 set nat enable
17 set srcaddr "all"

```

Close

Close

Internet Service database update occurs only if specific policy objects require a FortiGuard update - 7.4.1



This information is also available in the FortiManager 7.4 Administration Guide:

- [Adding offline model devices](#)

ZTP process has been optimized with Internet Service database update occurring only if specific objects used in the policy require a FortiGuard update.

To see when an ISDB update will be performed:

1. On FortiManager, go to the *Device Manager* and add a model device.

Add Device - Provide Model Device Info (1/2)

Add Model Device

Name

test-device-1

Link Device By ⓘ

Serial Number

Pre-shared Key

Serial Number

Use Device Blueprint

☐

Device Model

FortiGate-VM64

Port Provisioning

1

Enforce Firmware

☒ 7.4 (By Default)

Add to Device Group

☐

Add to Folder

☐

Pre-Run CLI Template

☐

Assign Policy Package

☒ default

Provisioning Templates

+

Metadata Variables

Edit Variable Mapping

Copy Device Dashboard

Click to select

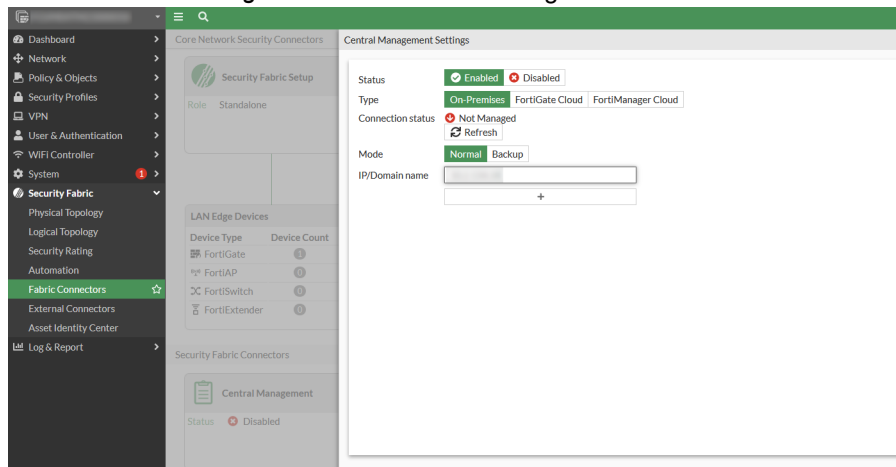
< Back

Next >

Cancel

2. Assign a Policy Package to the device.

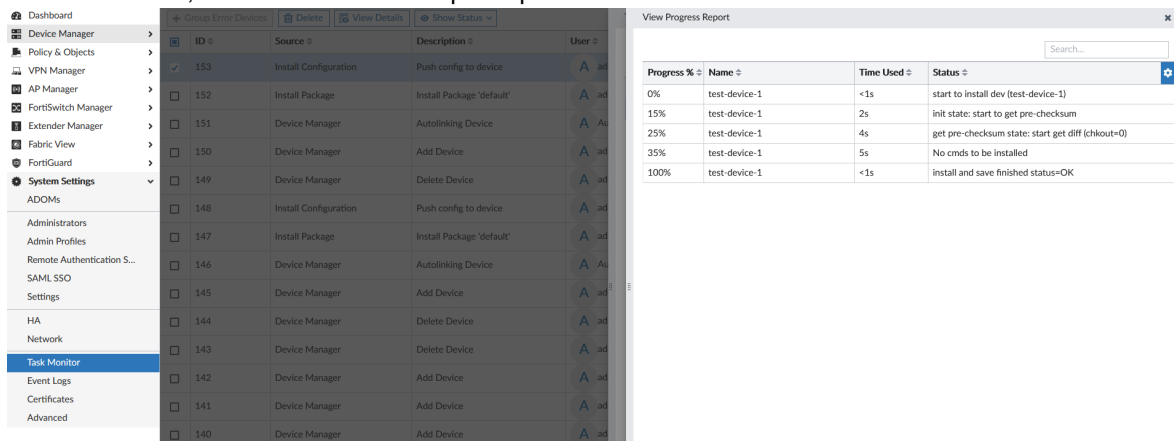
3. Enable *Central Management* from the FortiManager in the FortiGate GUI.



4. Following the device auto-link process, when the configuration is pushed to FortiGate, FortiManager determines if an ISDB update is required:

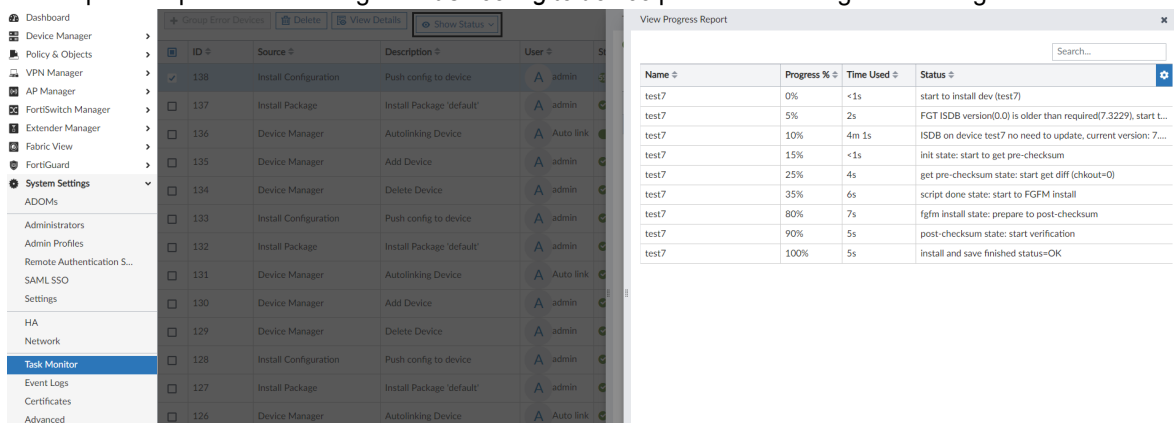
• ISDB update not required:

- If there is no Internet Service used in the Policy Package, there will be no ISDB update performed.
- If the Internet Service used in the Policy Package is the same version or an older version than the version on the FortiGate, there will be no ISDB update performed.



• ISDB update required:

- If the Internet Service used in the Policy Package is newer than the ISDB version on the FortiGate, an ISDB update is performed during the *Push config to device* process following auto-linking.



Policy and Objects

This section lists the new features added to FortiManager for policy and objects:

- [Policy on page 71](#)

Policy

This section lists the new features added to FortiManager for policies:

- [Install preview support for partial install on page 71](#)
- [Policy Package installation added link to the progress report page for installation errors on page 78](#)
- [Support for IoT Virtual Patching in NAC policies using pre-built severity filters on page 82](#)
- [Policy deletion warning message improved with selected policy number and name reference 7.4.1 on page 83](#)
- [Enable option for persistent policy hit-count on ADOM database 7.4.1 on page 84](#)
- [Partial install pushes only the instructed configuration \(JSON API\) 7.4.1 on page 85](#)
- [Policy partial install supports policy reorder/move operation \(JSON API\) 7.4.1 on page 87](#)

Install preview support for partial install



This information is also available in the FortiManager 7.4 Administration Guide:

- [Installing objects](#)

When the partial install feature is enabled, *Install Preview* can be used to view the configuration changes that will be made before a partial install.

To preview a partial install:

1. In the FortiManager CLI, enable partial install:

```
config system global
    set partial-install enable
end
```

2. Create an address a1.

Create New Firewall Address

Name

a1

Color

4

Type

Subnet

IP/Netmask

1.1.1.1/34

Resolve from name

Interface

any

Static Route Configuration

Comments

Add To Groups

Click to select

Advanced Options

Per-Device Mapping

Revision

Change Note*

d

Revision History

Revert

View Diff

Search...

	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note	
No record found.								

0

OK

Cancel

3. Use this address in a policy.

Create New Firewall Policy

ID

0

Name

Incoming Interface

any

x

+

Outgoing Interface

any

x

+

Source

a1

x

+

Negate Source

☐

IP/MAC Based Access Control

+

Destination

all

x

+

Negate Destination

☐

Service

ALL

x

+

Schedule

always

x

+

Action

Accept

Deny

IPSEC

Disclaimer Options

Block Notification

☐

Logging Options

Log Violation Traffic

☒

Advanced

WCCP

☐

Exempt from Captive Portal

☐

Comments

Advanced Options >

Revision

OK

Cancel

4. Install the policy to a FortiGate.
5. Modify the a1 address.

Edit Firewall Address

Name

a1

Color

4

Type

Subnet

IP/Netmask

1.1.1.2/255.255.255.255

Resolve from name

Interface

any

Static Route Configuration

Comments

Add To Groups

Click to select

Advanced Options

Per-Device Mapping

Revision

Change Note

0/1023

Revision History

Revert

View Diff

Search...

	Revision #	Changed by	Date/Time	Action	Change Note	
<input type="checkbox"/>	1	admin	2023-02-09 11:10:05	Create	d	<div></div>

1

OK

Cancel

6. Right click a1 and select *Install Object(s)*.

+ Create New + Edit Delete More...				View Search...			
Name	Type	Details	Interface	Comments	Created Time	Last Modified	Revision History
Address							
<input type="checkbox"/> none	Firewall Address	IP/Netmask: 0.0.0.0/255.255.255.255	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> login.microsoftonline.com	Firewall Address	FQDN:login.microsoftonline.com	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> login.microsoft.com	Firewall Address	FQDN:login.microsoft.com	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> login.windows.net	Firewall Address	FQDN:login.windows.net	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> gmail.com	Firewall Address	FQDN:gmail.com	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> wildcard.google.com	Firewall Address	FQDN:*google.com	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> wildcard.dropbox.com	Firewall Address	FQDN:*dropbox.com	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range: 10.212.134.200-10.212.134.210	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> all	Firewall Address	IP/Netmask: 0.0.0.0/0.0.0.0	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> FIREWALL_AUTH_PORTAL_ADDRESS	Firewall Address	IP/Netmask: 0.0.0.0/0.0.0.0	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> FABRIC_DEVICE	Firewall Address	IP/Netmask: 0.0.0.0/0.0.0.0	any	IPv4 addresses of Fabric Dev	admin / 2023-02-08 18:03:30		
<input type="checkbox"/> metadata-server	Firewall Address	IP/Netmask: 169.254.169.254/255.255.255.255	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> RFC1918-10	Firewall Address	IP/Netmask: 10.0.0.0/255.0.0.0	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> RFC1918-172	Firewall Address	IP/Netmask: 172.16.0.0/255.240.0.0	any		admin / 2023-02-08 18:03:30		
<input type="checkbox"/> RFC1918-192	Firewall Address	IP/Netmask: 192.168.0.0/255.255.0.0	any		admin / 2023-02-08 18:03:30		
<input checked="" type="checkbox"/> a1	Firewall Address	IP/Netmask: 1.1.1.2/255.255.255.255	any		admin / 2023-02-09 11:10:05	admin/2023-02-09 11:38:07	2
Address Group							
<input type="checkbox"/> G Suite	Address Group	gmail.com wildcard.google.com			admin / 2023-02-08 18:03:30		
<input type="checkbox"/> Microsoft Office 365	Address Group	login.microsoftonline.com login.microsoft.com login.windows.net			admin / 2023-02-08 18:03:30		
<input type="checkbox"/> RFC1918-GRP	Address Group	RFC1918-10 RFC1918-172 RFC1918-192			admin / 2023-02-08 18:03:30		
IPv6 Address							
<input type="checkbox"/> SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Address	IPv6 Subnet: ffff:ffff::120			admin / 2023-02-08 18:03:30		
<input type="checkbox"/> all	IPv6 Address	IPv6 Subnet: ::0			admin / 2023-02-08 18:03:30		
<input type="checkbox"/> none	IPv6 Address	IPv6 Subnet: ::128			admin / 2023-02-08 18:03:30		
IPv6 Address Group							
IPv6 Address Template							
Proxy Address							
<input type="checkbox"/> IPv6-address	Proxy Address	Host Regex Match: ^([0-9a-f]{0,4}){1,7}([0-9a-f]{1,4})?\$			admin / 2023-02-08 18:03:30		
<input type="checkbox"/> IPv4-address	Proxy Address	Host Regex Match: ^([0-9]{1-3}-[0-9]{1-3} [0-9]{1-3} 0-255-5-255)([0-9]{1-3} [0-9]{1-3} [0-9]{1-3} 0-255)?\$			admin / 2023-02-08 18:03:30		
Proxy Address Group							

7. Select the installation target and click *Install Preview*.
8. The install preview displays the pending configuration changes.



If you attempt to install an object that is not used in a policy, the device list displays *No record found*.

If you attempt to install an object with invalid configuration, *Install Preview* displays the configuration errors.



```
1 Copy device global objects
2
3 Copy objects for vdom root
4
5
6 Copy device global objects
7
8 Vdom copy failed:
9 error 131 - datasrc invalid. detail: copy datasrc failed, attr [associated-interface] value[a]
10
11
12 Copy objects for vdom root
13 "dynamic interface", "a", id=102, INVALID MAPPING - (null)
14 "firewall address", "a2", id=4442, INVALID MAPPING - datasrc invalid. detail: copy datasrc fai
15
16
17
18
19
```

Download Close

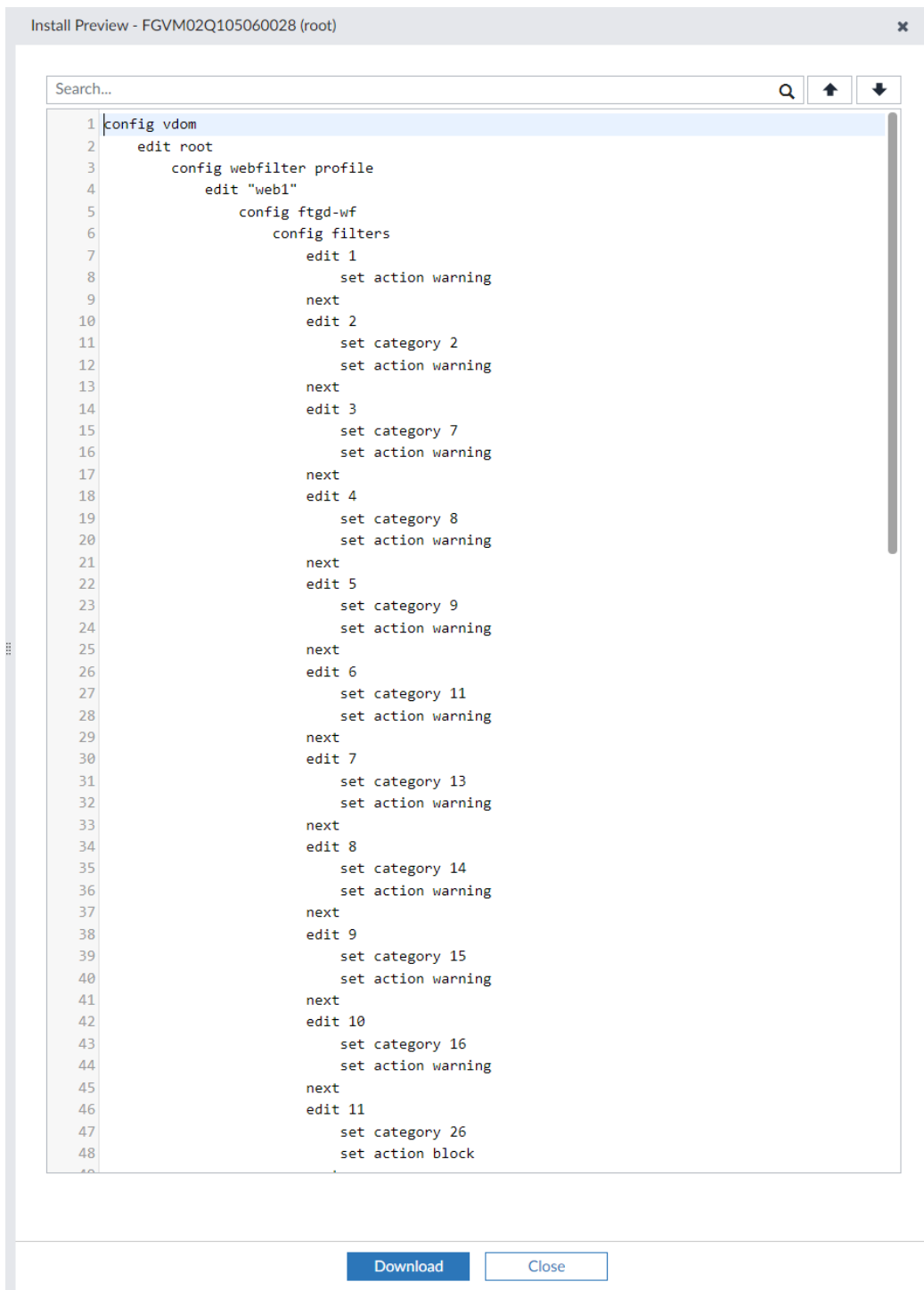
In *Install Preview*, metadata variables used in objects display the real value.



```
1 config vdom
2   edit root
3     config firewall address
4       edit "a2"
5         set uuid 7f1a7c0e-adbc-51ed-aefb-9e7c5acd66e7
6         set subnet 1.2.2.2 255.255.255.255
7       next
8     end
9   end
10
```

Download Close

Administrators with a restricted profile can use *Install Preview* for partial installs.



Policy Package installation added link to the progress report page for installation errors



This information is also available in the FortiManager 7.4 Administration Guide:

- [Installing policy packages and device settings](#)

When there is an error in policy and settings validation, you can view the progress report to see the specific error that occurred.

To view the progress report in the case of an install error:

1. Create a metadata variable `m1` with a default value of `1`.

Edit Metadata Variables

Name

m1

Description

Default Value

1

Per-Device Mapping >

Revision

Change Note*

0/1023

Revision History

Revert

View Diff

Search...

<input type="checkbox"/>	Revision #	Changed by	Date/Time	Action	Change Note	
<input type="checkbox"/>	1	admin	2023-02-08 17:01:45	Create	d	
						1

OK

Cancel

2. Create an address `a1` using the new metadata variable `m1` in it and bind the address to `portA`.

Edit Firewall Address

Name

a1

Color

4

Type

Subnet

IP/Netmask

\$(m1).1.1.1 255.255.255.0

Resolve from name

Interface

portA

Static Route Configuration

Comments

Add To Groups

Click to select

Advanced Options

Per-Device Mapping

Revision

Change Note*

0/1023

OK

Cancel

3. Create a policy with *Source* set to *a1* and *Incoming Interface* set to *portA*.

Edit Firewall Policy

ID

1

Name

Incoming Interface

portA

+

Outgoing Interface

any

+

Source

a1

+

Negate Source

☐

IP/MAC Based Access Control

+

Destination

all

+

Negate Destination

☐

Service

ALL

+

Schedule

always

+

Action

Accept

Deny

IPSEC

Disclaimer Options

Block Notification

☐

Logging Options

OK

Cancel

4. Launch *Install Wizard*. Select *Install Policy Package & Device Settings* and continue to the validation step. The *Install Wizard* displays an error message.

Install Wizard - Policy Package and Device Settings (default) (3/4)

✖ Task finished with errors.

Installation Preparation Total: 2/2, ✔ Success: 1, ⚠ Warning: 0, ✖ Error: 1 ⓘ Show Details 100%

View Progress Report Search...

#	Name	Time Used	Status
1	FGVM02Q105060028[copy] - root	<1s	Aborted due to previous error

1/2

✖ Interface Validation

The following ADOM interfaces have no mapping. All ADOM interfaces should be mapped before continue with installation.

Search...

<input type="checkbox"/>	Device Name	Unmapped Interface	Device Interface
<input type="checkbox"/>	FGVM02Q105060028(root)	portA	Click to select

1

< Back

Validation

Cancel

5. In the error message, click on *errors*.
The progress report displays with the error lines highlighted.

View Progress Report

Search...

Name	Progress %	Time Used	Status
FGVM02Q105060028[copy]	1%	<1s	Start copying policy to devdb, device(FGVM02Q105...
FGVM02Q105060028[copy]	1%	<1s	validation error on firewall policy 1, by dynamic interf...
FGVM02Q105060028[copy]	50%	<1s	vdom copy error: entry not exist. detail: Dynamic inte...
FGVM02Q105060028[copy]	100%	<1s	Copy rollbacked, due to error
FGVM02Q105060028[copy]	100%	<1s	Aborted due to previous error



Triple-click on a *Status* message to copy it and paste it to another document to read the full message.

Support for IoT Virtual Patching in NAC policies using pre-built severity filters

FortiManager includes support for IoT Virtual Patching in NAC policies using pre-built severity filters.



This information is also available in the FortiManager 7.4 Administration Guide:

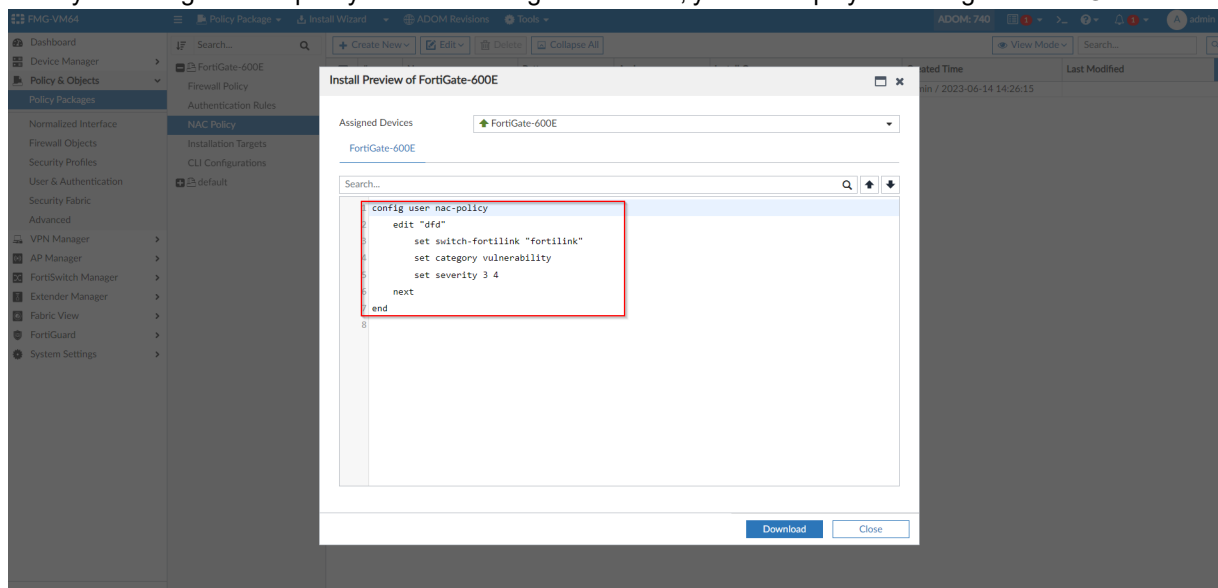
- [Create a new NAC policy](#)

To use IoT Virtual Patching in a NAC policy:

1. Go to *Policy & Objects > Policy Packages*, and create a new *NAC Policy*.
2. In the policy settings, select the *Vulnerability* category, then specify the *Severity* value (0 = Info, 1 = Low, 2 = Medium, 3 = High, 4 = Critical).

The screenshot shows the FortiManager 7.4.0 Administration Guide interface. The left sidebar displays the 'Policy & Objects' menu, with 'NAC Policy' selected under 'Policy Packages'. The main window shows the 'Edit NAC Policy' configuration. The 'Device Patterns' section has 'Category' set to 'Vulnerability' and 'Severity' set to '3'. The 'Switch Controller Action' section shows 'Assign VLAN' and 'Bounce Port' options. The 'Wireless Controller Action' section shows 'Assign VLAN' options. The 'Advanced Options' section is collapsed. The bottom of the window has 'OK' and 'Cancel' buttons.

3. Save your changes to the policy. After the changes are made, you can deploy the changes to FortiGate.



Policy deletion warning message improved with selected policy number and name reference - 7.4.1



This information is also available in the FortiManager 7.4 Administration Guide:

- [Editing policies](#)

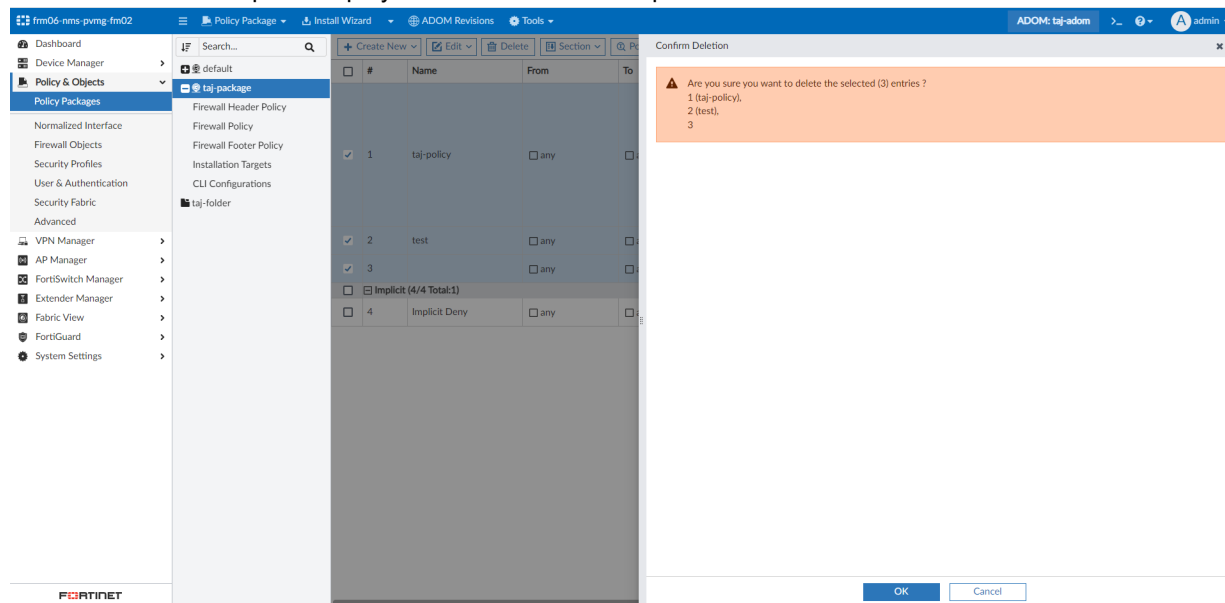
In FortiManager, the policy deletion warning message is improved with the selected policy number and name reference.

To view the confirmation when deleting a policy:

1. Go to *Policy & Objects > Policy Packages*.

2. Select a policy, and click *Delete* in the toolbar.

The *Confirm Deletion* pane displays information about the policies that will be deleted.



Enable option for persistent policy hit-count on ADOM database - 7.4.1



This information is also available in the FortiManager 7.4 Administration Guide:

- [Policy hit count](#)

In FortiManager 7.4.1, you can enable an option for a persistent policy hit-count on the ADOM database.

To save Last Used values on FortiManager:

1. In the FortiManager CLI, enter the following command to enable `save-last-hit-in-adomdb`.

```
config system global
set save-last-hit-in-adomdb enable
end
```

2. Enter the following command to view the "Last Used" timestamp value in the CLI.

```
exe fmpolicy print-adom-package <adom> <packageName> <policy-id>
```

3. Go to *Policy & Objects* > *Policy Packages*, and enable the *Last Used* column in *Column Settings*.

4. In the *Tools* dropdown, select *Refresh Hit Counts*.

In the following example, if the policy id 1002 hit count information (Hit Count/Packets/First Used/Last Used) are reset on the FortiGate side, 1002's "Last Used" value (2023/06/19 11:32) will *not* be cleared on FortiManager.

#	ID	From	To	Action	Hit Count	Packets	First Used	Last Used	Created Time	Last Modified
1	1002	port1	loopback002	Accept	0	0	2023/06/13 13:48	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
2	2002	port1	loopback002	Accept	2	14	2023/06/13 13:48	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
3	1003	port1	loopback003	Accept	2	4	2023/06/13 13:48	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
4	2003	port1	loopback003	Accept	2	14	2023/06/13 13:48	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
5	1004	port1	loopback004	Accept	1	2	2023/06/19 11:32	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
6	2004	port1	loopback004	Accept	1	7	2023/06/19 11:32	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
7	1005	port1	loopback005	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
8	2005	port1	loopback005	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
9	1006	port1	loopback006	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
10	2006	port1	loopback006	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
11	1007	port1	loopback007	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
12	2007	port1	loopback007	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
13	1008	port1	loopback008	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
14	2008	port1	loopback008	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
15	1009	port1	loopback009	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
16	2009	port1	loopback009	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
17	1010	port1	loopback010	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
18	2010	port1	loopback010	Accept	3	22	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
19	1011	port1	loopback011	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
20	2011	port1	loopback011	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
21	1012	port1	loopback012	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
22	2012	port1	loopback012	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
23	1013	port1	loopback013	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
24	2013	port1	loopback013	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
25	1014	port1	loopback014	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
26	2014	port1	loopback014	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
27	1015	port1	loopback015	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
28	2015	port1	loopback015	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:19	admin
29	1016	port1	loopback016	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:20	admin
30	2016	port1	loopback016	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:20	admin
31	1017	port1	loopback017	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:20	admin
32	2017	port1	loopback017	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:20	admin
33	1018	port1	loopback018	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:20	admin
34	2018	port1	loopback018	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:20	admin
35	1019	port1	loopback019	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:20	admin
36	2019	port1	loopback019	Accept	3	21	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:20	admin
37	1020	port1	loopback020	Accept	3	6	2023/05/31 23:15	2023/06/19 11:32	admin / 2023-06-14 16:30:20	admin

The next time *Refresh Hit Counts* is clicked, if a non-blank value is received as the new "Last Used" timestamp that is more recent than the stored value (2023/06/19 11:32), it will be updated and displayed.

Partial install pushes only the instructed configuration (JSON API) - 7.4.1

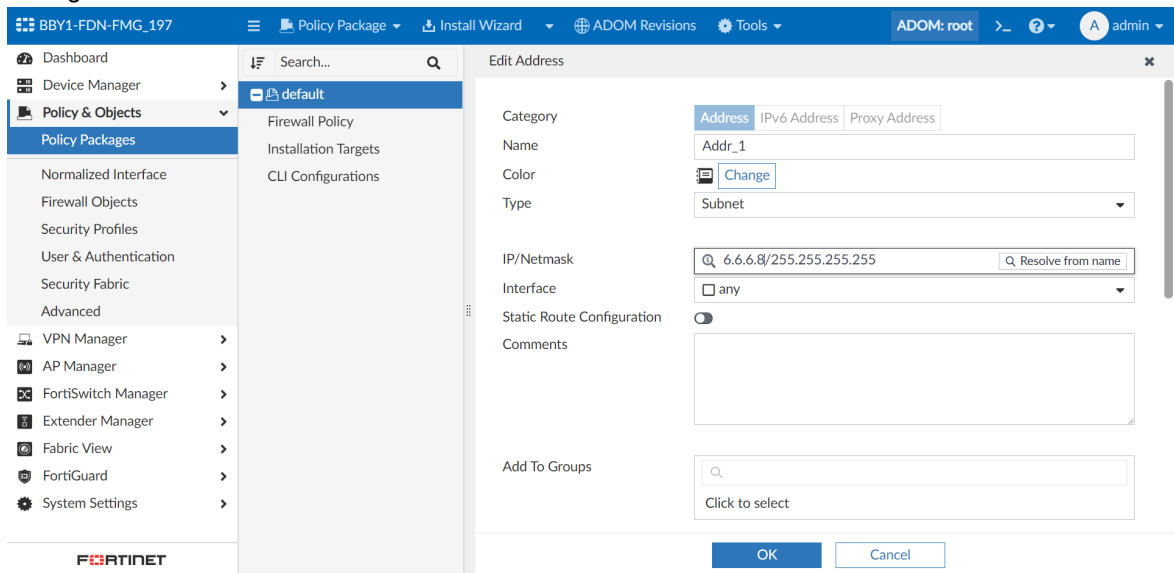
FortiManager 7.4.1 supports partial installs to push only the instructed configuration (using JSON API) without other pending changes on the device database to better address the role separation between different admin types.

Example of a partial install using JSON API

- Make changes to the managed device. In this example, two changes are made:
 - Change the device *Idle Timeout* setting:
 - Go to *Device Manager > Device & Groups* and edit a managed device.
 - In *System Settings*, change the device *Idle Timeout* setting to 471.

The screenshot shows the FortiManager interface for a managed device (BBY1-FDN-FMG_197). The left sidebar shows the navigation menu with 'Device Manager' expanded. The main content area shows the 'System Settings' configuration page. Under 'Administration Settings', the 'Idle Timeout' is set to 471 minutes. The 'Apply' button is visible at the bottom right.

- b. Change an address in *Policy & Objects*.
 - i. Go to *Policy & Objects > Policy Packages* and edit a policy package.
 - ii. Change an address to 6.6.6.8/32.



2. Using the FortiManager JSON API, perform a partial install. In this example, only the changes to the address are specified.

```
{
  "method": "exec",
  "params": [
    {
      "data": {
        "adom": "root",
        "objects": [
          ["update", "obj/firewall/address/Addr_1", "", ""]
        ],
        "flags": 0
      },
      "url": "securityconsole/install/objects/v2"
    }
  ],
  "session":
  "4Itgh5MwczfkFt9xmpYZcKVhc0iLvcjWV5XP17lyjxwhEDEIkP4HscHfCdk68yx7p7RGILVkcLAY8QHcc3jl+A="
}

{
  "result": [
    {
      "data": {
        "task": 22
      },
    },
  ],
}
```

```
    "status": {  
        "code": 0,  
        "message": "OK"  
    },  
    "url": "securityconsole/install/objects/v2"  
}  
]  
}
```

3. The install log shows only the address change was installed as intended. The change to the *Idle Timeout* setting was not installed.

```
Start installing  
FortiGate-VM64 $ config vdom  
FortiGate-VM64 (vdom) $ edit root  
current vf=root:0  
FortiGate-VM64 (root) $ config firewall address  
FortiGate-VM64 (address) $ edit "Addr_1"  
FortiGate-VM64 (Addr_1) $ set subnet 6.6.6.8 255.255.255.255  
FortiGate-VM64 (Addr_1) $ next  
FortiGate-VM64 (address) $ end  
FortiGate-VM64 (root) $ end  
---> generating verification report  
<--- done generating verification report  
install finished
```

Policy partial install supports policy reorder/move operation (JSON API) - 7.4.1

Policy partial install (JSON API) supports policy reorder/move operation.

Example of a reorder/move operation in partial installs using JSON API

1. In this example, seven policies and address `Addr_1` are created in a Policy Package.

The screenshot shows the FortiManager interface for Policy & Objects. The left sidebar lists various management sections, with 'Policy & Objects' selected. The main area displays a table of Firewall Policies. The table has columns for #, Name, From, To, and Source. Policies 1 through 7 are listed, each with a checkbox in the # column. Policy 8 is an 'Implicit Deny' policy. The source for policy 1 is 'Addr_1', and for policies 2 through 7, it is 'all'. The table also shows a summary row for 'Implicit (8/8 Total:1)'.

#	Name	From	To	Source
<input type="checkbox"/> 1	1	<input type="checkbox"/> any	<input type="checkbox"/> any	Addr_1
<input type="checkbox"/> 2	2	<input type="checkbox"/> any	<input type="checkbox"/> any	all
<input type="checkbox"/> 3	3	<input type="checkbox"/> any	<input type="checkbox"/> any	all
<input type="checkbox"/> 4	4	<input type="checkbox"/> any	<input type="checkbox"/> any	all
<input type="checkbox"/> 5	5	<input type="checkbox"/> any	<input type="checkbox"/> any	all
<input type="checkbox"/> 6	6	<input type="checkbox"/> any	<input type="checkbox"/> any	all
<input type="checkbox"/> 7	7	<input type="checkbox"/> any	<input type="checkbox"/> any	all
Implicit (8/8 Total:1)				
<input type="checkbox"/> 8	Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	all

2. Install the policies to a FortiGate.

The screenshot shows the FortiManager interface for Policy & Objects, specifically the 'Firewall Policy' section. The left sidebar lists various management sections, with 'Firewall Policy' selected. The main area displays a table of Firewall Policies. The table has columns for Name, From, To, Source, Destination, Schedule, Service, Action, IP Pool, NAT, Type, and Security P. Policies 1 through 7 are listed, each with a checkbox in the Name column. Policy 1 is 'Addr_1', and for policies 2 through 7, it is 'all'. The source for policy 1 is 'Addr_1', and for policies 2 through 7, it is 'all'. The table also shows a summary row for 'Implicit (1)'.

Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security P
<input type="checkbox"/> 1	<input type="checkbox"/> any	<input type="checkbox"/> any	all	Addr_1	always	ALL	DENY			Standard	SSL no-ir
<input type="checkbox"/> 2	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	DENY			Standard	SSL no-ir
<input type="checkbox"/> 3	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	DENY			Standard	SSL no-ir
<input type="checkbox"/> 4	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	DENY			Standard	SSL no-ir
<input type="checkbox"/> 5	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	DENY			Standard	SSL no-ir
<input type="checkbox"/> 6	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	DENY			Standard	SSL no-ir
<input type="checkbox"/> 7	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	DENY			Standard	SSL no-ir
Implicit (1)											

3. Perform the following modifications on the Policy Package.
 - a. Create one new policy and move it before policy 1.
 - b. Change `Addr_1` IP.
 - c. Move policy 6 after policy 3.

d. Delete policy 4.

#	Name	From	To	Source
1	8	any	any	all
2	1	any	any	Addr_1
3	2	any	any	all
4	3	any	any	all
5	6	any	any	all
6	4	any	any	all
7	5	any	any	all
8	7	any	any	all
Implicit (9/9 Total:1)				
9	Implicit Deny	any	any	all

4. Using JSON API, perform a partial install.

Post:

```
{
  "method": "exec",
  "params": [
    {
      "data": {
        "adom": "root",
        "objects": [
          ["add", "pkg/default/firewall/policy/9", "before", "1"],
          ["update", "obj/firewall/address/Addr_1", "", ""],
          ["delete", "pkg/default/firewall/policy/4", "", ""],
          ["move", "pkg/default/firewall/policy/6", "after", "3"]
        ],
        "flags": 0
      },
      "url": "securityconsole/install/objects/v2"
    }
  ],
  "session":
    "msWfmFWGIJyDX/LRYaOPFALvGjgjJ82yzV2s919g1DWgVY1r1HFJu1o4+xsOQCSdA0kyiSwB5DrXs12rW0vEmw="
}
```

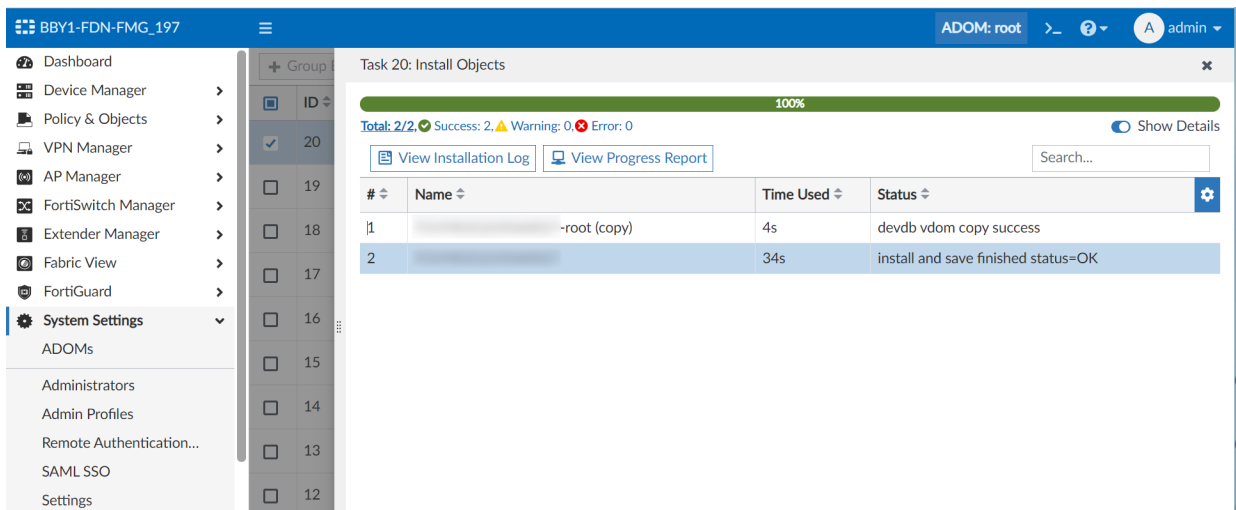
Response:

```
{
  "result": [
    {
      "data": {
        "task": 20
      },
      "status": {
        "code": 0,
        "message": "OK"
      }
    }
  ]
}
```

```

    "url": "securityconsole/install/objects/v2"
  }
]
}

```



5. View the install log.

View Install Log

Starting log (Run on device)

Start installing

```
FortiGate-VM64 $ config vdom
```

```
FortiGate-VM64 (vdom) $ edit root
```

```
current vf=root:0
```

```
FortiGate-VM64 (root) $ config firewall policy
```

```
FortiGate-VM64 (policy) $ delete 4
```

```
FortiGate-VM64 (policy) $ end
```

```
FortiGate-VM64 (root) $ config firewall address
```

```
FortiGate-VM64 (address) $ edit "Addr_1"
```

```
FortiGate-VM64 (Addr_1) $ set subnet 6.6.6.7 255.255.255.255
```

```
FortiGate-VM64 (Addr_1) $ next
```

```
FortiGate-VM64 (address) $ end
```

```
FortiGate-VM64 (root) $ config firewall policy
```

```
FortiGate-VM64 (policy) $ edit 9
```

```
FortiGate-VM64 (9) $ set name "8"
```

```
FortiGate-VM64 (9) $ set uuid 798858d0-2506-51ee-2c43-da0bf419ad7d
```

```
FortiGate-VM64 (9) $ set srcintf "any"
```

```
FortiGate-VM64 (9) $ set dstintf "any"
```

```
FortiGate-VM64 (9) $ set srcaddr "all"
```

```

FortiGate-VM64 (9) $ set dstaddr "all"
FortiGate-VM64 (9) $ set schedule "always"
FortiGate-VM64 (9) $ set service "ALL"
FortiGate-VM64 (9) $ set logtraffic all
FortiGate-VM64 (9) $ next
FortiGate-VM64 (policy) $ move 9 before 1
FortiGate-VM64 (policy) $ move 5 after 6
FortiGate-VM64 (policy) $ end
FortiGate-VM64 (root) $ end

---> generating verification report
<--- done generating verification report

install finished

```

6. All changes are installed to the FortiGate.

Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security P
Uncategorized 7											
8	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY			Standard	SSL no-ir
1	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> Addr_1	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY			Standard	SSL no-ir
2	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY			Standard	SSL no-ir
3	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY			Standard	SSL no-ir
6	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY			Standard	SSL no-ir
5	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY			Standard	SSL no-ir
7	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY			Standard	SSL no-ir
Implicit 1											

System

This section lists the new features added to FortiManager for system settings:

- [High Availability \(HA\) on page 92](#)
- [ADOM on page 93](#)
- [Others on page 99](#)

High Availability (HA)

This section lists the new features added to FortiManager for high availability (HA):

- [FortiManager supports different VM type platforms to form the FortiManager cluster on page 92](#)

FortiManager supports different VM type platforms to form the FortiManager cluster



This information is also available in the FortiManager 7.4 Administration Guide:

- [High Availability](#)

FortiManager supports different VM type platforms to form the FortiManager cluster.

Below is an example of a FortiManager HA formed with FMG-VM64-KVM as the Primary device and FMG-VM64 as the secondary. The steps to configure HA have not changed.

- For the Primary HA device:

Cluster Status

Refresh

Search...

SN	Mode	IP	Sync Status	Enable	Module Data Synchronized	Pending Module Data
FMG-VM0A17002226	Secondary	10.2.106.64	✓	✓	0.0 KB	0.0 KB
FMG-VMTM22006258	Primary	10.3.144.35	✓		0.0 KB	0.0 KB

Cluster Settings

Failover Mode

Manual

VRRP

Operation Mode

Standalone

Primary

Secondary

Peer IP and Peer SN

IP Type	Peer IP	Peer SN	Action
IPv4	10.2.106.64	FMG-VM0A17002226	<div>✕</div> <div>+</div>

Cluster ID

1

(1-64)

Group Password

File Quota

4096

MB (2048-20480)

Heart Beat Interval

10

Seconds

Fallover Threshold

30

(1-255)

VIP

VRRP Interface

Click to select

Priority

1

(1-253)

Unicast

☐

Monitored IP

IP	Interface	Action
	Click to select	<div>✕</div> <div>+</div>

Download Debug Log

Download

Apply

- For the Secondary HA device:

Cluster Status
Refresh
Search...

SN	Mode	IP	Sync Status	Enable	Module Data Synchronized	Pending Module Data
FMG-VM0A17002226	Secondary	10.3.106.64	✓		0.0 KB	0.0 KB
FMG-VMTM22006258	Primary	10.2.144.35	✓		0.0 KB	0.0 KB

Cluster Settings

Fallover Mode
Operation Mode
Peer IP and Peer SN
Cluster ID
Group Password
File Quota
Heart Beat Interval
Failover Threshold
VIP
VRRP Interface
Priority
Unicast
Monitored IP
Download Debug Log

Manual
VRRP

Standalone
Primary
Secondary

IP Type
Peer IP
Peer SN
Action

IPv4
10.2.144.35
FMG-VMTM22006258
✕

Cluster ID
1
(1-64)

Group Password

File Quota
4096
MB (2048-20480)

Heart Beat Interval
10
Seconds

Failover Threshold
30
(1-255)

VIP

VRRP Interface
Click to select

Priority
1
(1-253)

Unicast

Monitored IP
IP
Interface
Action

Click to select
✕
+

Download Debug Log
Download

Apply

ADOM

This section lists the new features added to FortiManager for ADOMs:

- ADOM 7.2 Policy Package supports installation on FortiGate 7.4 7.4.1 on page 93
- 7.2 ADOM managing mixed FOS versions 7.4.1 on page 96
- FortiManager can upgrade multiple ADOMs (same version) at the same time 7.4.1 on page 98

ADOM 7.2 Policy Package supports installation on FortiGate 7.4 - 7.4.1



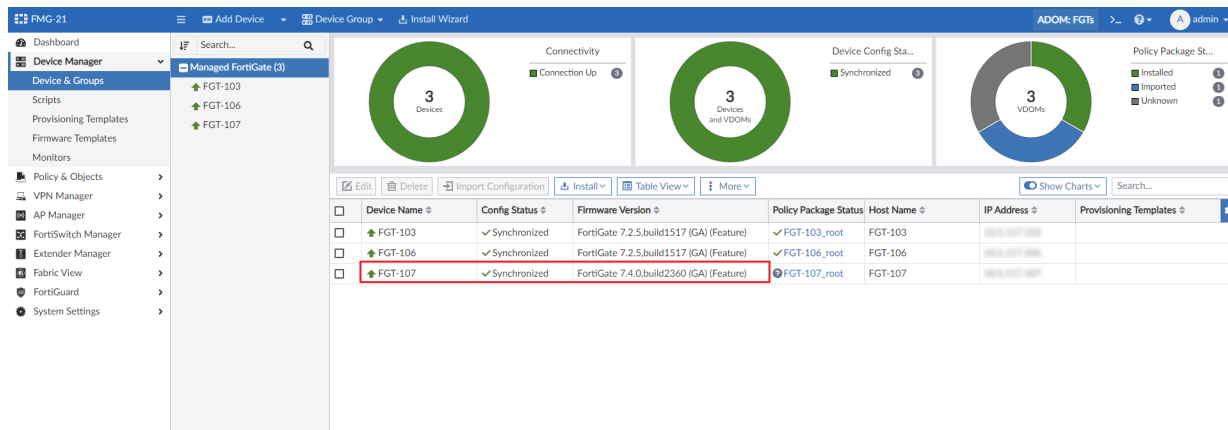
This information is also available in the FortiManager 7.4 Administration Guide:

- [Using Mixed Versions in ADOMs](#)

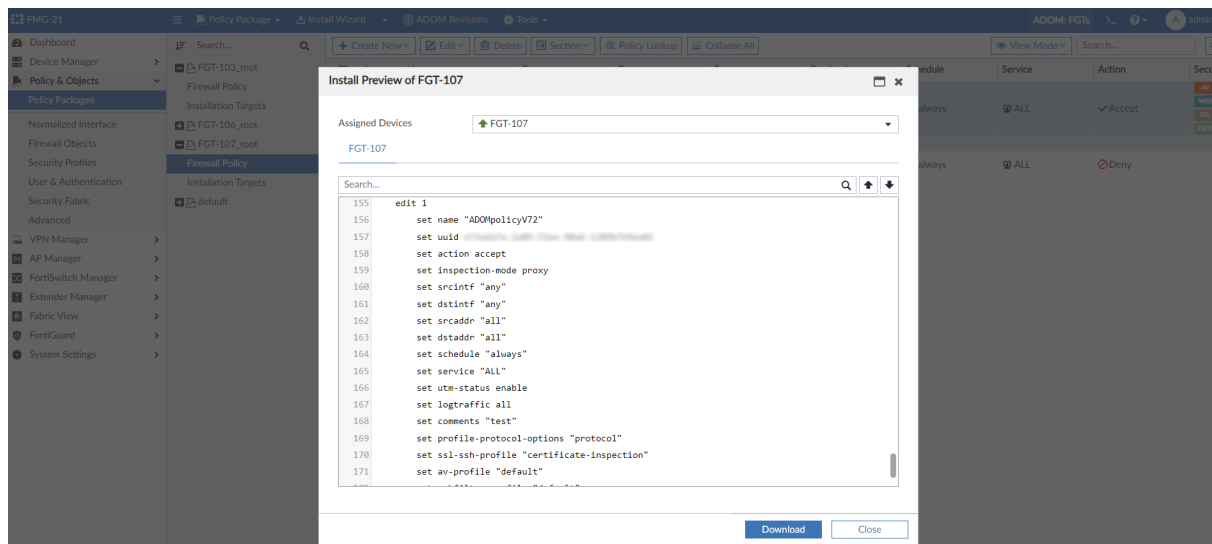
FortiManager ADOM 7.2 Policy Packages support installation on FortiGates on version 7.4.

- ADOMs on version 7.2 are normally used to manage FortiGate devices on version 7.2 but in some cases you may need to upgrade some managed FortiGate units in the ADOM from 7.2 to 7.4. FortiManager can install 7.2 policy

packages to FortiGate 7.4 devices.

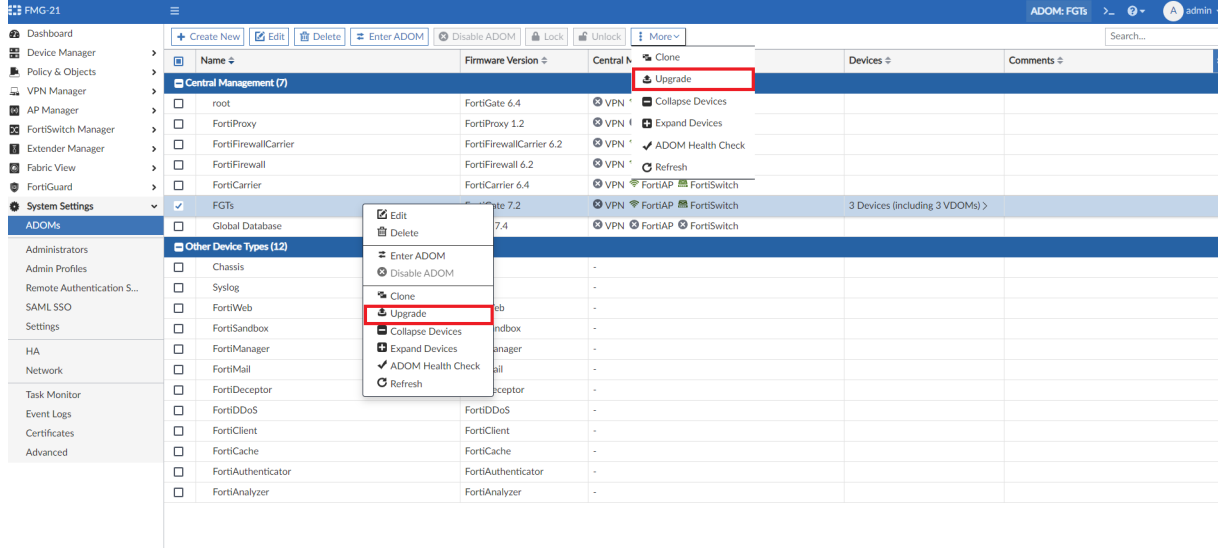


- When you create a firewall policy in a 7.2 ADOM and install it to a FortiGate 7.4 device, FortiManager's backend system automatically handles the 7.4 syntax. FortiManager doesn't change any new 7.4 features on the FortiGate 7.4 unit.

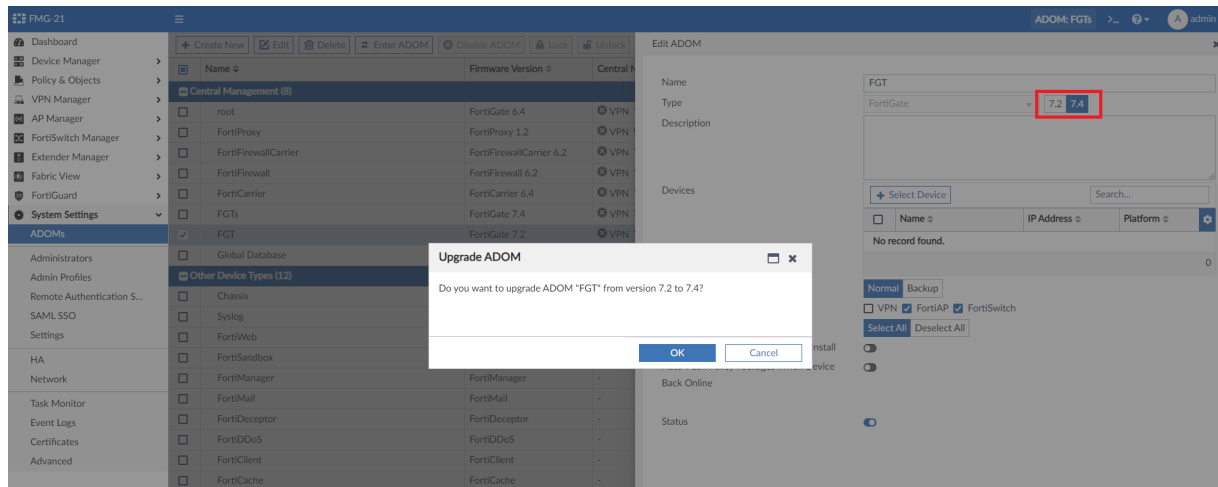


There are three ways to upgrade an ADOM from version 7.2 to 7.4:

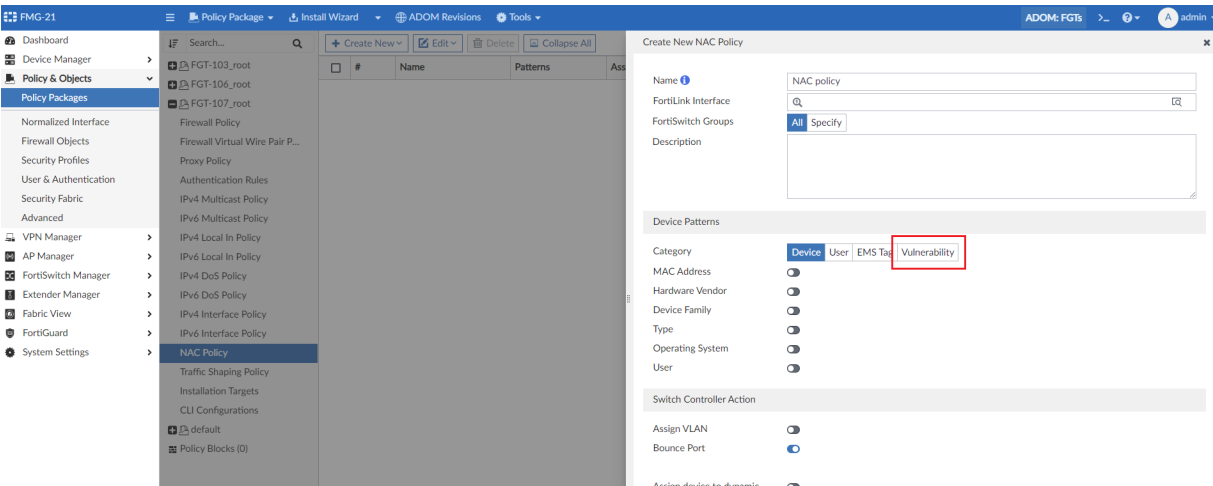
1. Navigate to *System Settings > ADOMs > More > Upgrade*.
2. Right-Click the ADOM and select *Upgrade*.



3. Edit the ADOM to select to the next version 7.4.



After upgrading the ADOM from 7.2 to 7.4, all of the database objects are automatically converted to the 7.4 format and the GUI reflects new 7.4 features.



7.2 ADOM managing mixed FOS versions - 7.4.1

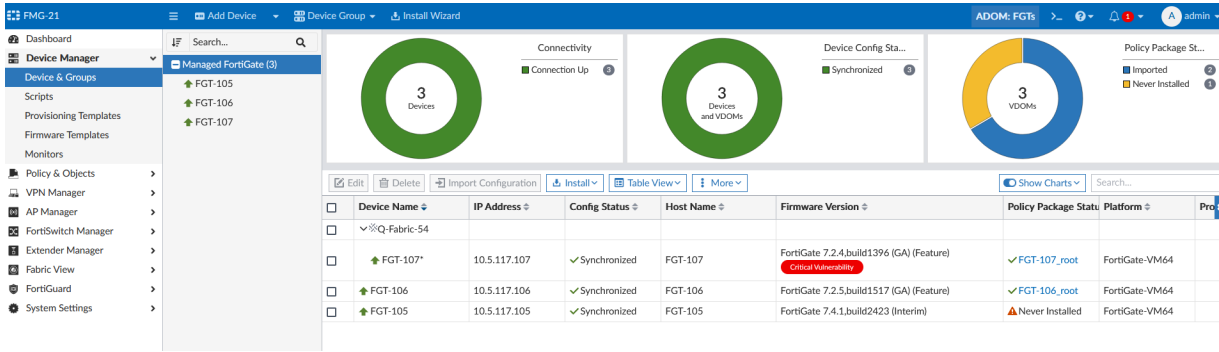


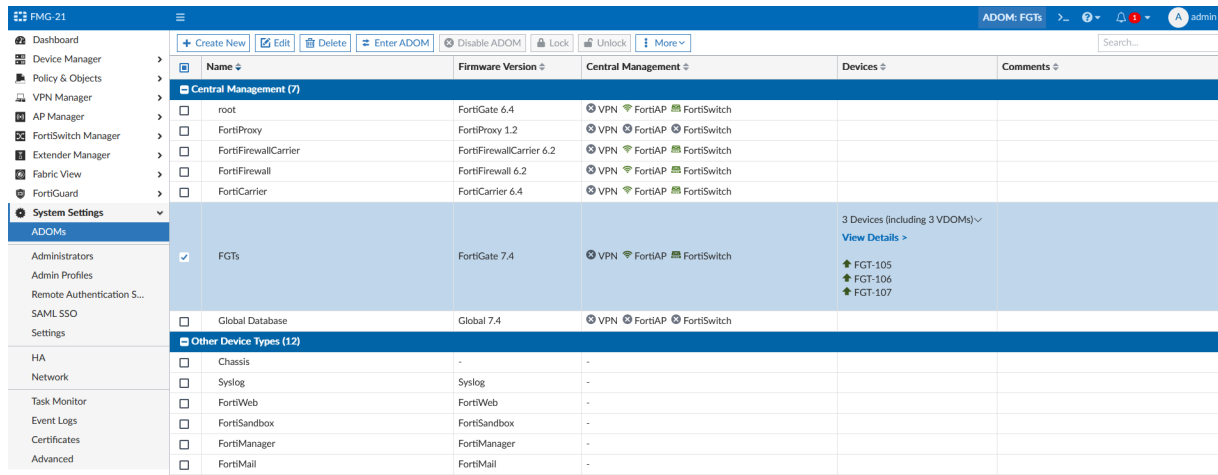
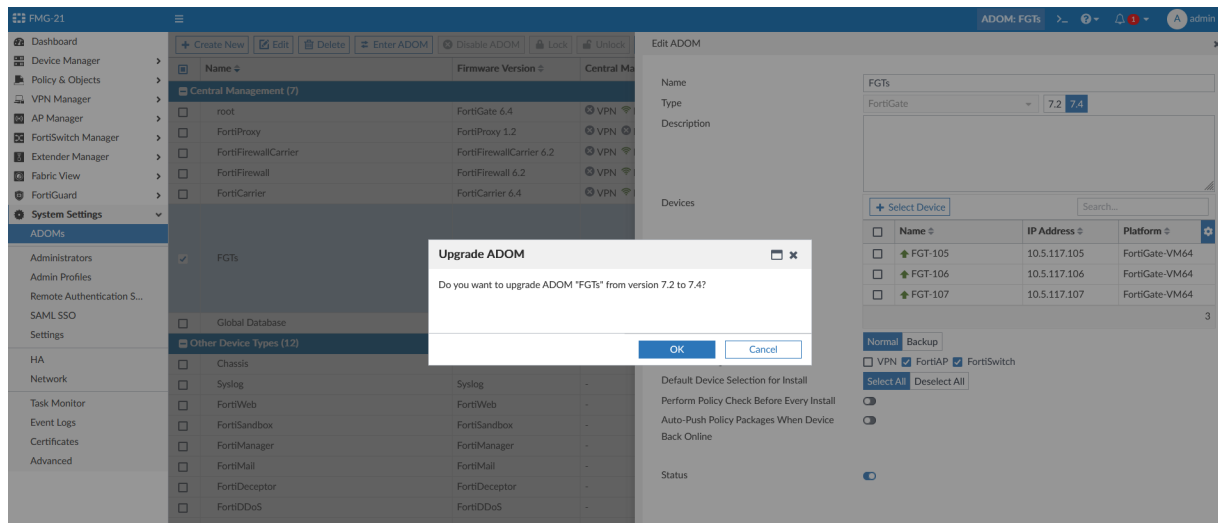
This information is also available in the FortiManager 7.4 Administration Guide:

- [Using Mixed Versions in ADOMs](#)

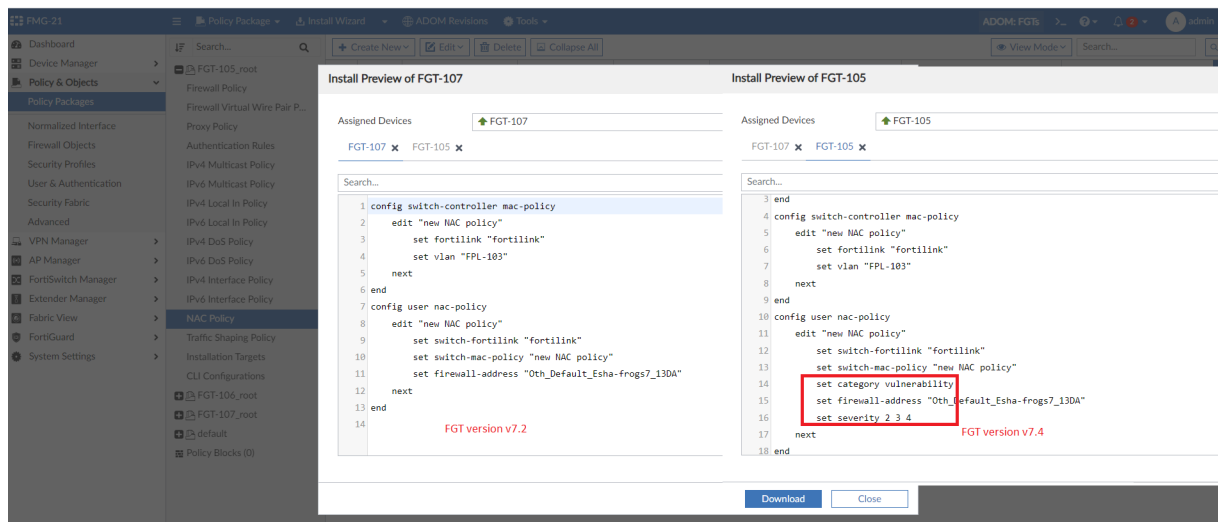
When a 7.2 ADOM is managing mixed FOS versions (FortiOS 7.2 and 7.4), the ADOM can be upgraded to version 7.4.

- When FortiManager is managing mixed FortiGate units running on FortiOS 7.2 and FortiOS 7.4 in an 7.2 ADOM, FortiManager allows you to upgrade the ADOM from 7.2 to 7.4 before upgrading all FortiGates in the ADOM to FortiOS 7.4.





- In the upgraded 7.4 ADOM, you can create new 7.4 firewall policies and install the policy to both FortiGate devices on FortiOS 7.4 and 7.2. FortiManager's backend system automatically downgrades the 7.4 syntax to the 7.2 version when installed to a FortiOS 7.2 device.



FortiManager can upgrade multiple ADOMs (same version) at the same time - 7.4.1



This information is also available in the FortiManager 7.4 Administration Guide:

- [Upgrading an ADOM](#)

FortiManager is able to upgrade multiple ADOMs on the same version at the same time.

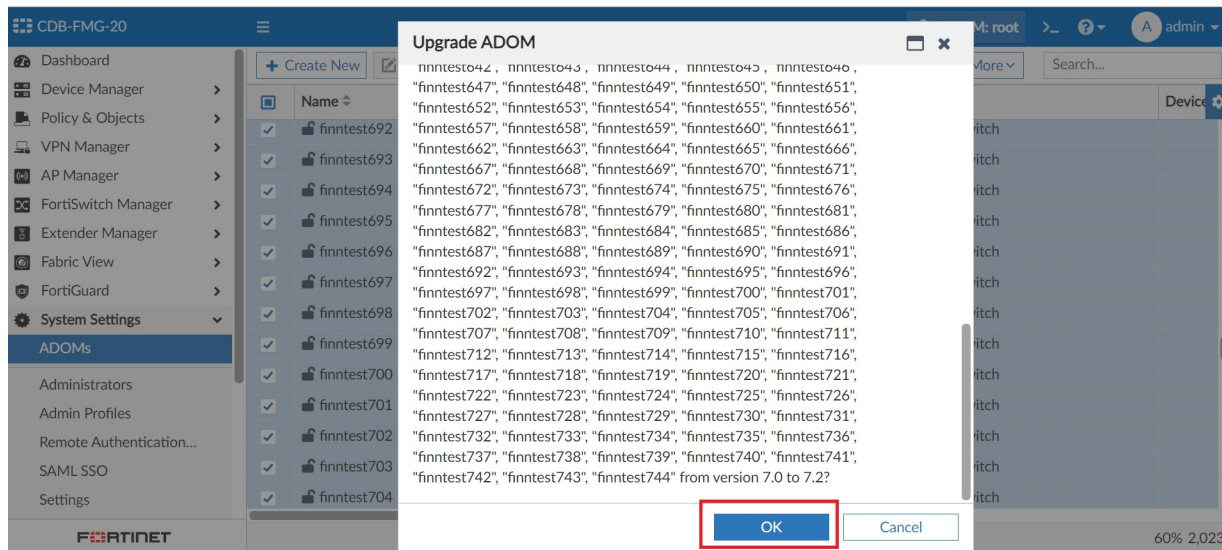
To upgrade multiple ADOMs at the same time:

1. Go to *System Settings > ADOMs*.
2. Select multiple ADOMs of the same version in the ADOM table and do one of the following:
 - a. Right-click on a selected device in the table and select *Upgrade*.
 - b. Select *More > Upgrade* in the toolbar.

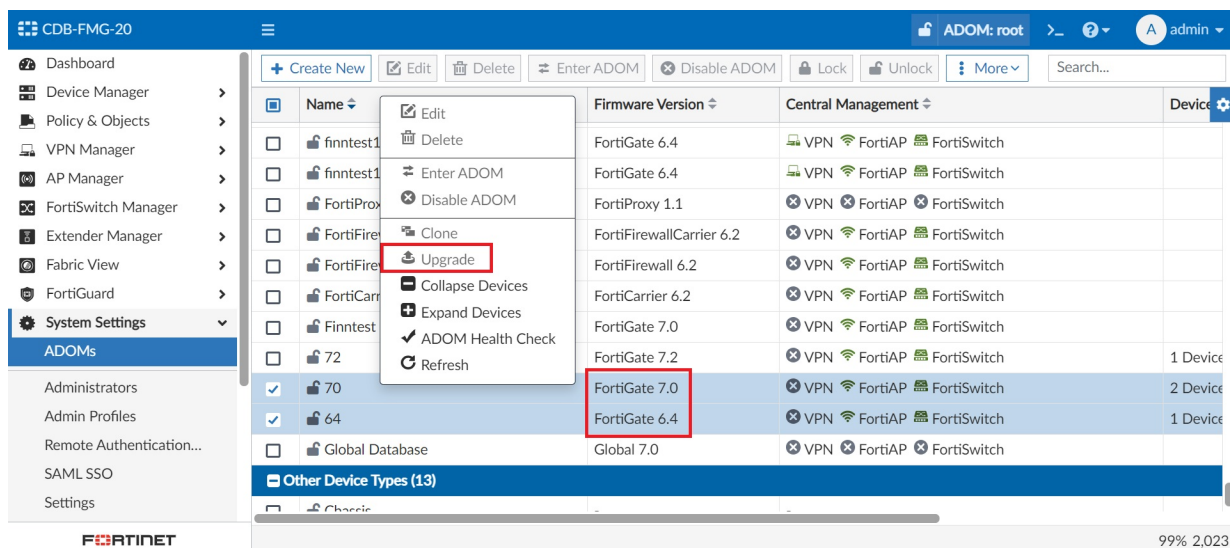
In this example, the customer has 200 ADOMs and they want to upgrade their ADOMs at the same time. Each ADOM is on version 7.0 and has one managed FortiGate device. FortiManager can upgrade all of the ADOMs at the same time.

The screenshot shows the FortiManager interface with the 'ADOMs' tab selected in the left sidebar. The main table displays a list of ADOMs. A context menu is open over the table, with the 'Upgrade' option highlighted. The table has columns for Name, Firmware Version, Central Management, and Devices. The 'Firmware Version' column for all visible ADOMs is 'FortiGate 7.0'. The 'Central Management' column shows various FortiManager components like VPN, FortiAP, and FortiSwitch. The 'Devices' column shows a list of managed devices for each ADOM.

Name	Firmware Version	Central Management	Devices
finntest599	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest600	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest601	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest602	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest603	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest604	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest605	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest606	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest607	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest608	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest609	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest610	FortiGate 7.0	VPN, FortiAP, FortiSwitch	
finntest611	FortiGate 7.0	VPN, FortiAP, FortiSwitch	



In this example, the customer has one ADOM on 7.0 and another on 6.4. When both ADOMs are selected, the upgrade button is unavailable because the ADOMs are on different versions. The ADOMs cannot be upgraded at the same time.



Others

This section lists the new features added to FortiManager for other features relating to system settings:

- Block out contract device from upgrading to next or major or minor release on page 100
- Automatic system backup setup in GUI to configure a backup schedule and visualize backup history 7.4.1 on page 102

Block out contract device from upgrading to next or major or minor release



This information is also available in the FortiManager 7.4 Administration Guide:

- [Updating the system firmware.](#)

To view available FortiGuard images:

1. A FortiManager with a valid contract will display all available FortiGuard images and allow upgrading or downgrading to any version.

- System Settings:

The screenshot shows the 'Firmware Management' window in FortiManager. The 'Current Version' is v7.0.3-build1362 230210 (Interim). The 'Upload Firmware' section has a button that says 'Add files by drag & drop here or [Add Files](#)'. The 'FortiGuard Firmware' section shows a dropdown menu with '7.2.2 (1334)' selected. Below the dropdown is a search bar and a list of available versions: 7.2.2 (1334), 7.2.1 (1215), 7.2.0 (1124), 7.0.4 (306), 7.0.3 (254), 7.0.2 (180), 6.4.10 (2549), and 6.4.9 (2513). The 'Backup Configuration' and 'Encryption' sections are empty. At the bottom right are 'OK' and 'Cancel' buttons.

2. A FortiManager without a valid contract or with an expired contract will only display available patch images and support patch upgrades.

- System Settings:

Firmware Management

Current Version

v7.0.3-build0237 230215 (Interim)

Upload Firmware

Add files by drag & drop here or [Add Files](#)

FortiGuard Firmware

7.0.4 (306)

Backup Configuration

Q

Encryption

✓ 7.0.4 (306)

7.0.3 (254)

7.0.2 (180)


OK


Cancel

- FortiManager setup wizard:

FortiManager Setup - Upgrade Firmware (3/4)

Upgrade Firmware

 A new firmware version is available

Current Version	v7.0.2-build0180 230209 (Interim)
Latest Version	7.0.4 (306)
 Release Notes	
Backup Configuration	<input checked="" type="checkbox"/>
Encryption	<input type="checkbox"/>

Next >

Later

Automatic system backup setup in GUI to configure a backup schedule and visualize backup history - 7.4.1



This information is also available in the FortiManager 7.4 Administration Guide:

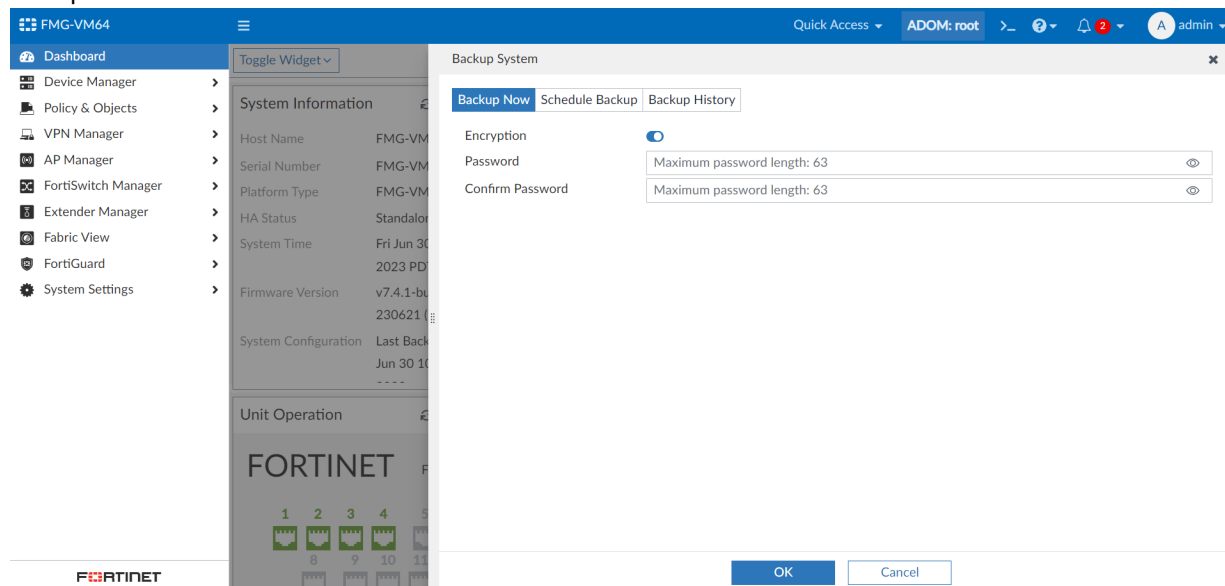
- [Backing up the system](#)

Automatic system backup setup is available in the FortiManager GUI to configure a backup schedule and visualize the backup history.

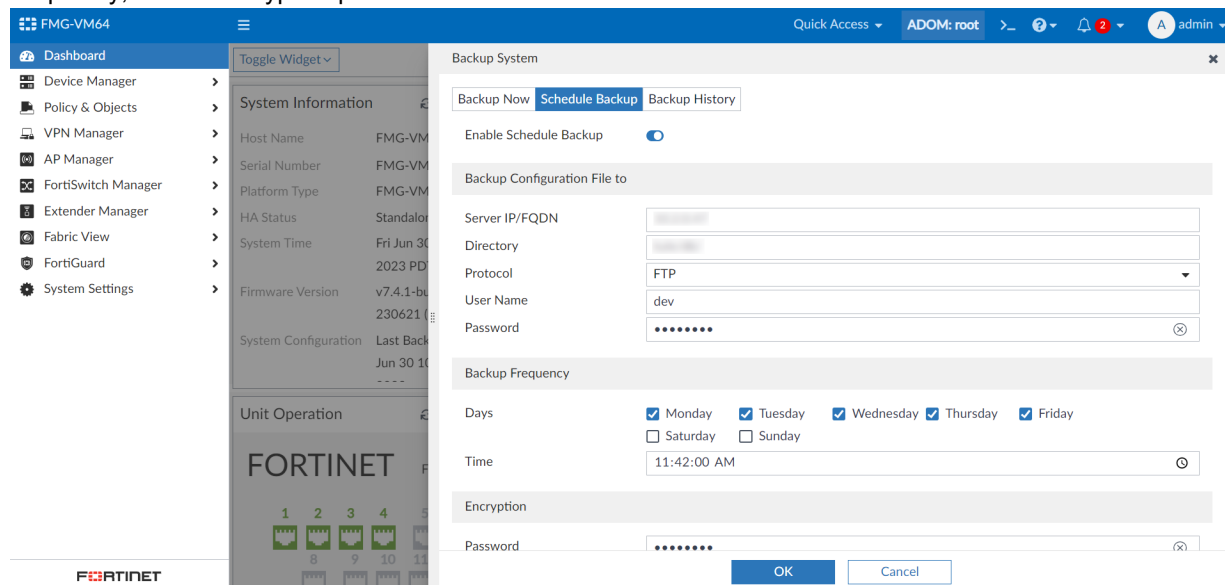
To configure scheduled backups and view backup history in the GUI:

1. Go to *Dashboard*.

- In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens.



- Select the *Schedule Backup* tab.
- Enable the *Enable Schedule Backup* option, and configure the options including the backup location, backup frequency, and an encryption password.



- Click **OK**.

6. Select the *Backup History* tab.

The backup history displays the *Date & Time*, *Admin*, *Size* and *Status* of each backup.

Backup System

Backup Now | Schedule Backup | **Backup History**

Search...

Date & Time	Admin	Size	Status
Fri Jun 30 12:01:50 2023	admin	226.4 MB	Success
Fri Jun 30 11:42:02 2023	Scheduled	226.4 MB	Success
Fri Jun 30 10:12:23 2023	test1	226.4 MB	Success
Fri Jun 30 09:55:51 2023	admin	226.4 MB	Success
Fri Jun 30 09:50:45 2023	(null)	226.4 MB	Success
Fri Jun 30 09:50:26 2023	(null)	0.0 KB	Success
Fri Jun 30 09:49:15 2023	(null)	226.4 MB	Success
Fri Jun 30 09:48:59 2023	(null)	0.0 KB	Success
Fri Jun 30 09:25:16 2023	test2	260.9 MB	Success
Thu Jun 29 15:41:14 2023	(null)	260.9 MB	Success
Thu Jun 29 15:40:54 2023	(null)	0.0 KB	Success

0% 16

Close

Cloud Services

This section lists the new features added to FortiManager for cloud services:

- [FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS on page 105](#)

FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS

FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS.



This information is also available in the FortiManager 7.4 Administration Guide:

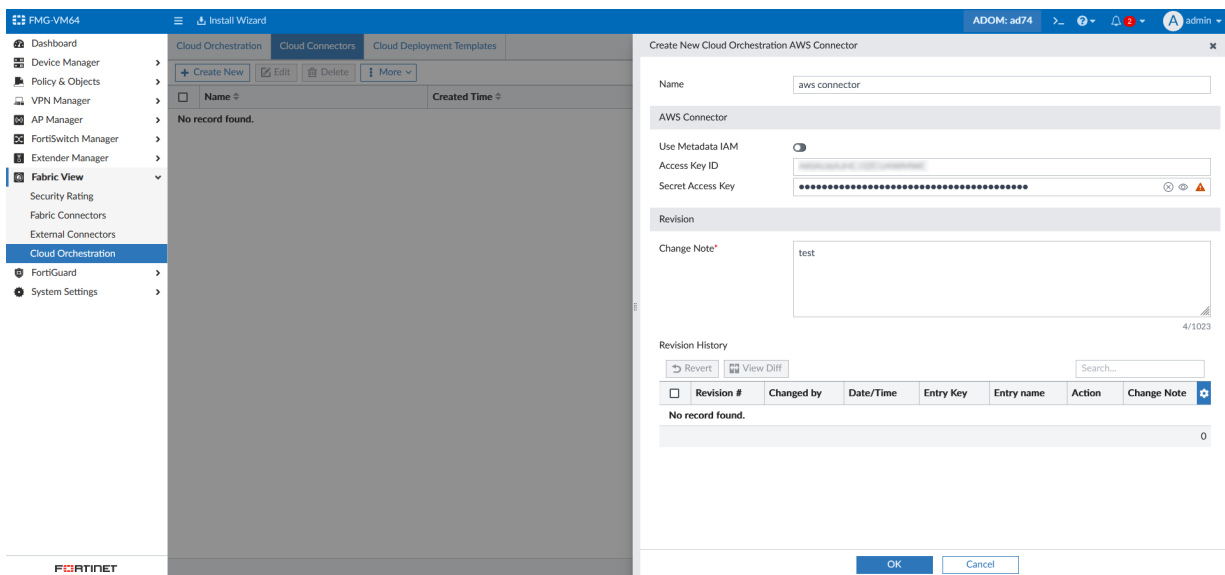
- [Cloud Orchestration](#)
-

FortiManager *Fabric View* adds Cloud Orchestration with the following panes:

- Cloud Orchestration
- Cloud Connectors
- Cloud Deployment Templates

To configure cloud orchestration using FortiManager:

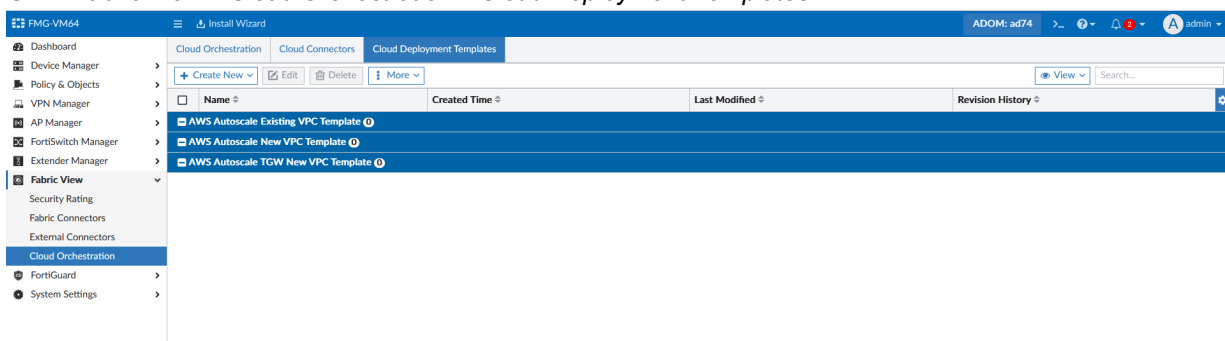
1. Create an AWS cloud orchestration connector:
 - a. Go to *Fabric View* > *Cloud Orchestration* > *Cloud Connectors*.
 - b. Click *Create New*.
 - c. Configure the AWS connector to connect to your AWS server.
You can enable *Use Metadata IAM* for FortiManager AWS instances using IAM.



d. Click OK.

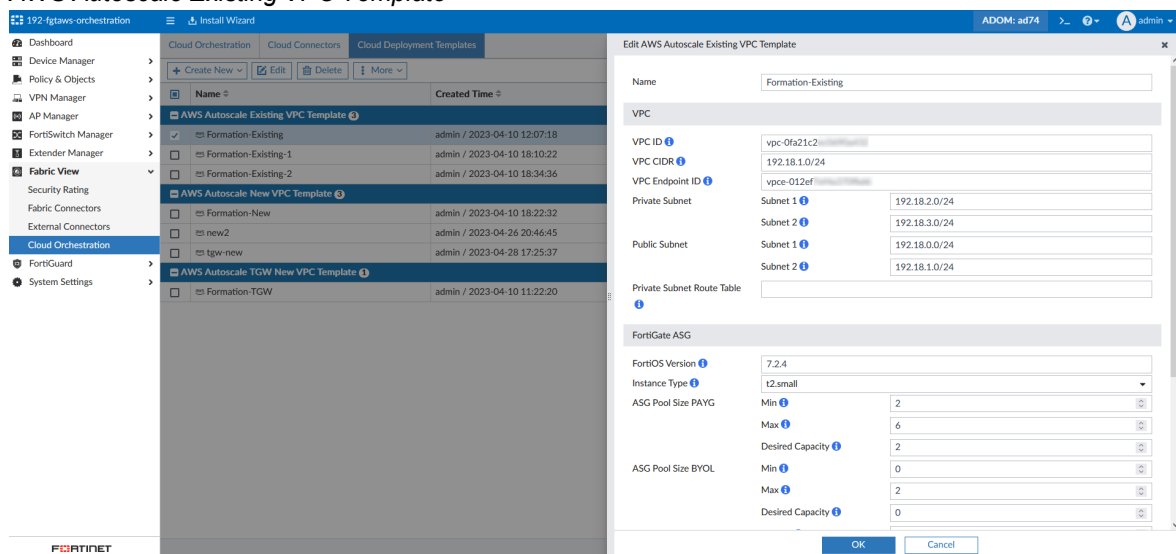
2. Create a cloud deployment template:

a. Go to *Fabric View > Cloud Orchestration > Cloud Deployment Templates*.



b. Click Create New, and select a deployment template type. There are three template types available:

i. *AWS Autoscale Existing VPC Template*



ii. AWS Autoscale New VPC Template

The screenshot shows the FortiManager interface with the 'Edit AWS Autoscale New VPC Template' window open. The left sidebar shows the navigation menu with 'Cloud Orchestration' selected. The main panel displays a table of templates and a detailed configuration form for the 'tgw-new' template.

Name	Created Time
AWS Autoscale Existing VPC Template	
Formation-Existing	admin / 2023-04-10 12:07:18
Formation-Existing-1	admin / 2023-04-10 18:10:22
Formation-Existing-2	admin / 2023-04-10 18:34:36
AWS Autoscale New VPC Template	
Formation-New	admin / 2023-04-10 18:22:32
new2	admin / 2023-04-26 20:46:45
tgw-new	admin / 2023-04-28 17:25:37
AWS Autoscale TGW New VPC Template	
Formation-TGW	admin / 2023-04-10 11:22:20

Edit AWS Autoscale New VPC Template

Name: tgw-new

VPC

VPC CIDR: 192.168.0.0/16

Private Subnet

CIDR 1: 192.168.2.0/24

CIDR 2: 192.168.3.0/24

Public Subnet

CIDR 1: 192.168.0.0/24

CIDR 2: 192.168.1.0/24

FortiGate ASG

FortiOS Version: 7.2.4

Instance Type: c5.xlarge

ASG Pool Size PAYG

Min: 2

Max: 6

Desired Capacity: 2

ASG Pool Size BYOL

Min: 2

Max: 2

Desired Capacity: 2

Threshold

Scale In: 25

Scale out: 80

FortiGate Admin

CIDR: 0.0.0.0/0

Port: 8443

OK Cancel

iii. AWS Autoscale TGW New VPC Template

The screenshot shows the FortiManager interface with the 'Edit AWS Autoscale TGW New VPC Template' window open. The left sidebar shows the navigation menu with 'Cloud Orchestration' selected. The main panel displays a table of templates and a detailed configuration form for the 'Formation-TGW' template.

Name	Created Time
AWS Autoscale Existing VPC Template	
Formation-Existing	admin / 2023-04-10 12:07:18
Formation-Existing-1	admin / 2023-04-10 18:10:22
Formation-Existing-2	admin / 2023-04-10 18:34:36
AWS Autoscale New VPC Template	
Formation-New	admin / 2023-04-10 18:22:32
new2	admin / 2023-04-26 20:46:45
tgw-new	admin / 2023-04-28 17:25:37
AWS Autoscale TGW New VPC Template	
Formation-TGW	admin / 2023-04-10 11:22:20

Edit AWS Autoscale TGW New VPC Template

Name: Formation-TGW

VPC

VPC CIDR: 192.168.0.0/16

Public Subnet

CIDR 1: 192.168.0.0/24

CIDR 2: 192.168.1.0/24

FortiGate ASG

FortiOS Version: 7.2.4

Instance Type: c5.xlarge

ASG Pool Size PAYG

Min: 2

Max: 6

Desired Capacity: 2

ASG Pool Size BYOL

Min: 0

Max: 2

Desired Capacity: 0

Threshold

Scale In: 10

Scale out: 40

FortiGate Admin

CIDR: 0.0.0.0/0

Port: 8443

Transit Gateway

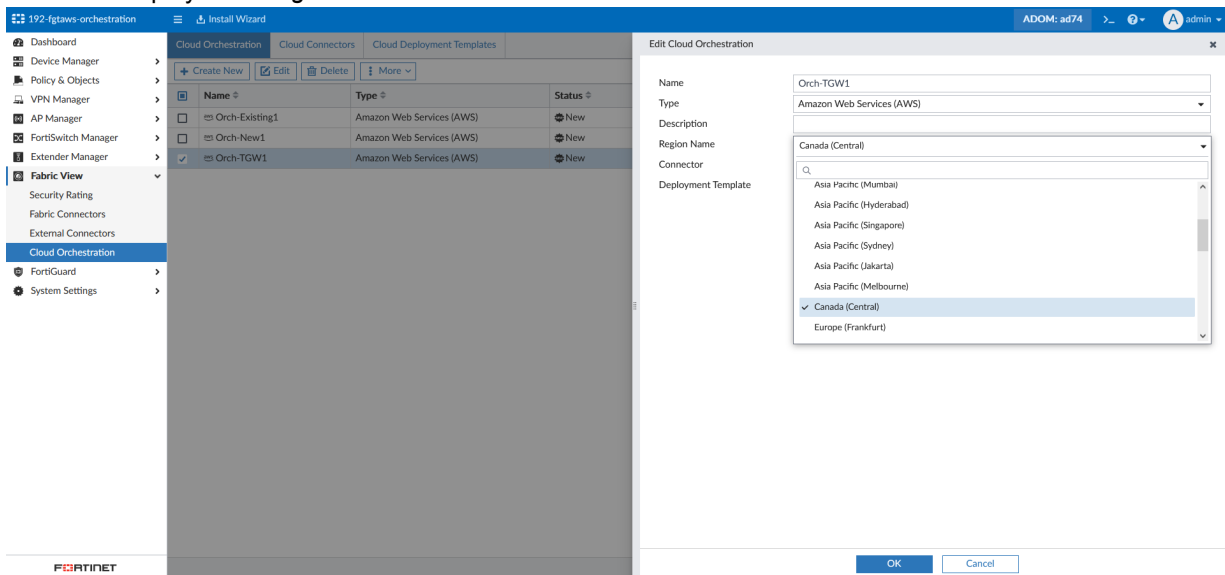
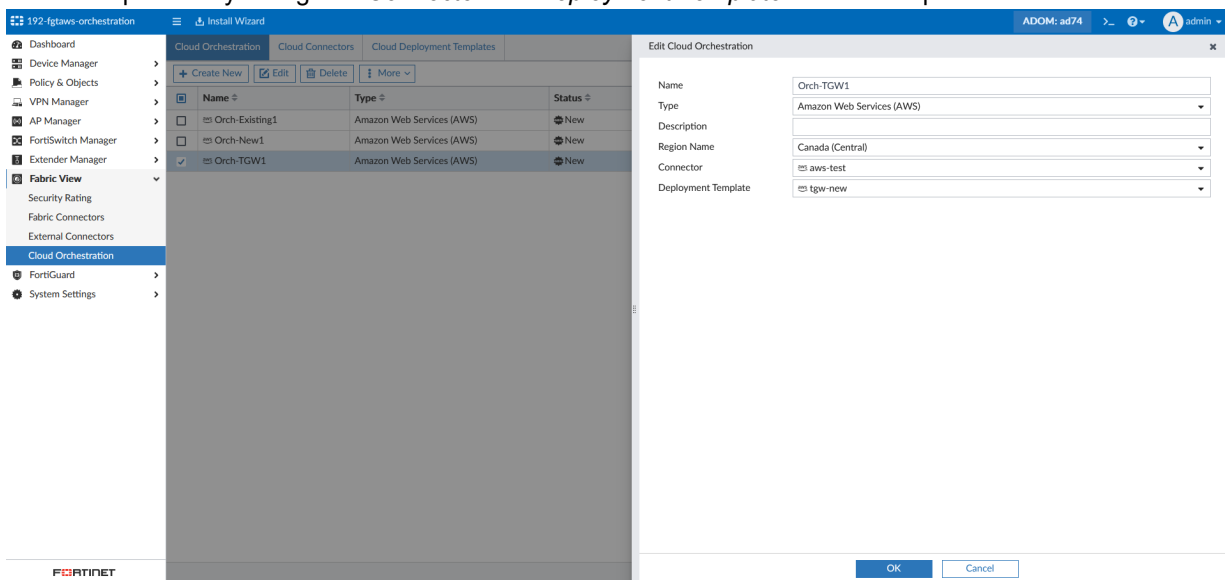
OK Cancel

- c. Configure the details for your chosen template, including the virtual private cloud (VPC) and FortiGate autoscale group (ASG) settings.

- d. Click OK.

3. Configure cloud orchestration:

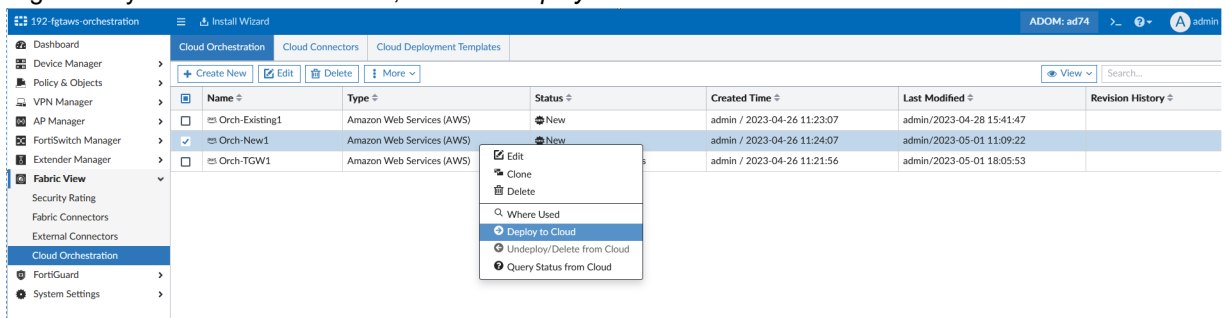
- a. Go to *Fabric View > Cloud Orchestration > Cloud Orchestration*.
- b. Click *Create New*.
- c. Enter a *Name* and optional *Description* for your cloud orchestration.

d. Select the deployment *Region*.e. Select the previously configured *Connector* and *Deployment Template* from the dropdown menus.

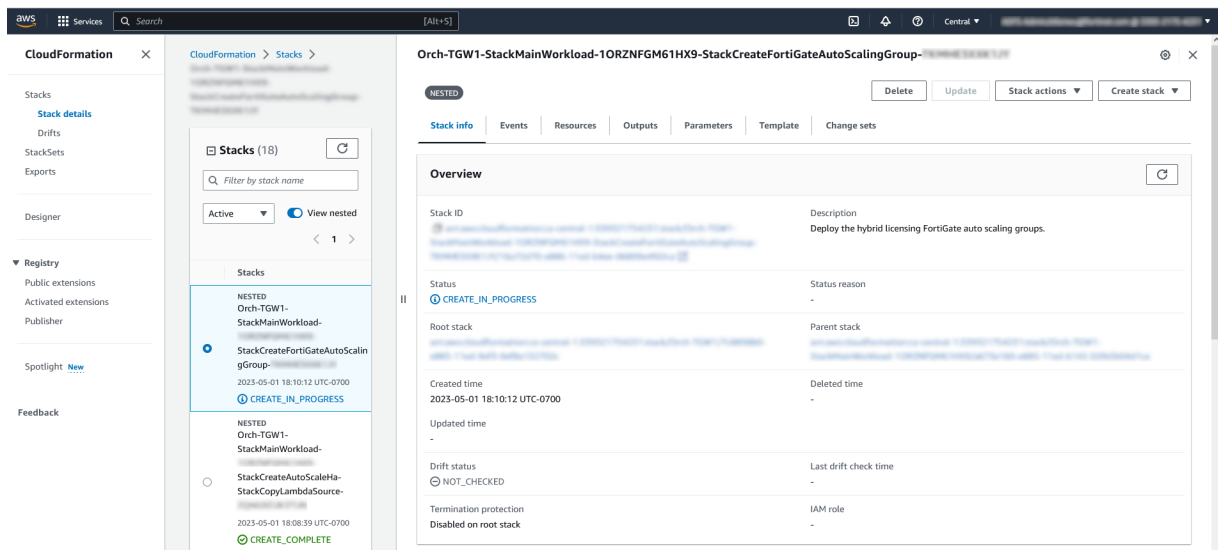
f. Click OK.

4. Deploy to cloud:

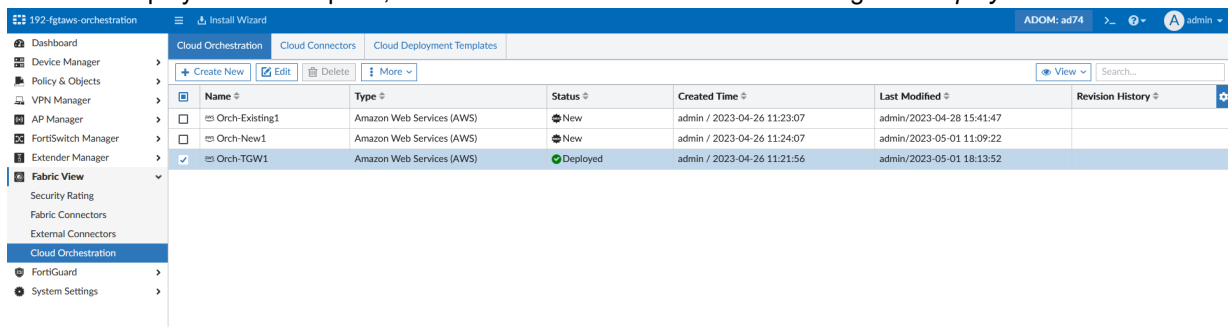
- Go to *Fabric View > Cloud Orchestration > Cloud Orchestration*.
- Right click your cloud orchestration, and click *Deploy to Cloud*.



AWS CloudFormation shows the deploy as *CREATE_IN_PROGRESS*.

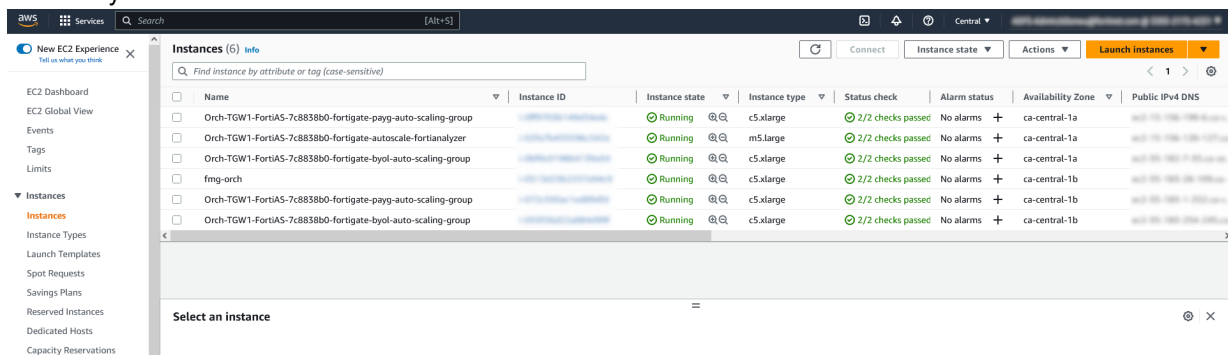


When the deployment is complete, the status of the cloud orchestration changes to *Deployed*.



Check on AWS EC2 to confirm the instances are deployed as expected.

In this example the cloud orchestration has deployed 2 FortiGate BYOL, 2 FortiGate PAYG, and 1 FortiAnalyzer.



Compare the settings with the FortiManager Cloud Deployment template to confirm the settings match.

The screenshot shows the FortiManager 7.4.0 interface. The left sidebar contains the following menu items: Dashboard, Device Manager, Policy & Objects, VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, Fabric View (expanded), Security Rating, Fabric Connectors, External Connectors, Cloud Orchestration (selected), FortiGuard, and System Settings. The main panel is titled '192-igtaws-orchestration' and shows a table of templates under the 'Cloud Deployment Templates' tab. The table has columns for Name and Created Time. The selected template is 'AWS Autoscale New VPC Template'. The right panel shows the configuration for this template, including fields for FortiOS Version, Instance Type, ASG Pool Size PAYG, ASG Pool Size BYOL, Threshold, FortiGate Admin, and FortiAnalyzer options.

Name	Created Time
AWS Autoscale Existing VPC Template	
Formation-Existing	admin / 2023-04-10 12:07:18
Formation-Existing-1	admin / 2023-04-10 18:10:22
Formation-Existing-2	admin / 2023-04-10 18:34:36
AWS Autoscale New VPC Template	
Formation-New	admin / 2023-04-10 18:22:32
new2	admin / 2023-04-26 20:46:45
tpw-new	admin / 2023-04-28 17:25:37
AWS Autoscale TGW New VPC Template	
Formation-TGW	admin / 2023-04-10 11:22:20

Edit AWS Autoscale New VPC Template

FortiOS Version: 7.2.4
Instance Type: c5.xlarge
ASG Pool Size PAYG: Min: 2, Max: 6, Desired Capacity: 2
ASG Pool Size BYOL: Min: 2, Max: 2, Desired Capacity: 2
Threshold: Scale In: 25, Scale out: 80
FortiGate Admin: CIDR: 0.0.0.0/0, Port: 8443
Misc: Autoscale Notification Subscriber Email:
Advanced Options: FortiAnalyzer Integration Options: ☐ FortiAnalyzer Version: 7.2.0, Instance Type: m5.large

OK Cancel

Other

This section lists other new features added to FortiManager:

- [New FortiManager UX design on page 111](#)
- [Fabric and External connector pages have been reorganized for an enhanced user experience on page 121](#)
- [FortiManager connector relay to AWS will proxy all individual FortiGate requests on page 125](#)
- [Fabric and External connector pages have been reorganized for an enhanced user experience on page 121](#)
- [FortiManager imports EPGs entries using the Cisco ACI connector as individual objects on page 140](#)

New FortiManager UX design



This information is also available in the FortiManager 7.4 Administration Guide:

- [GUI Overview](#)

In FortiManager 7.4.0, there is a new FortiManager user experience design that allows for per-admin customizable dashboards and adds a 3-layer left navigation menu to increase accessibility.

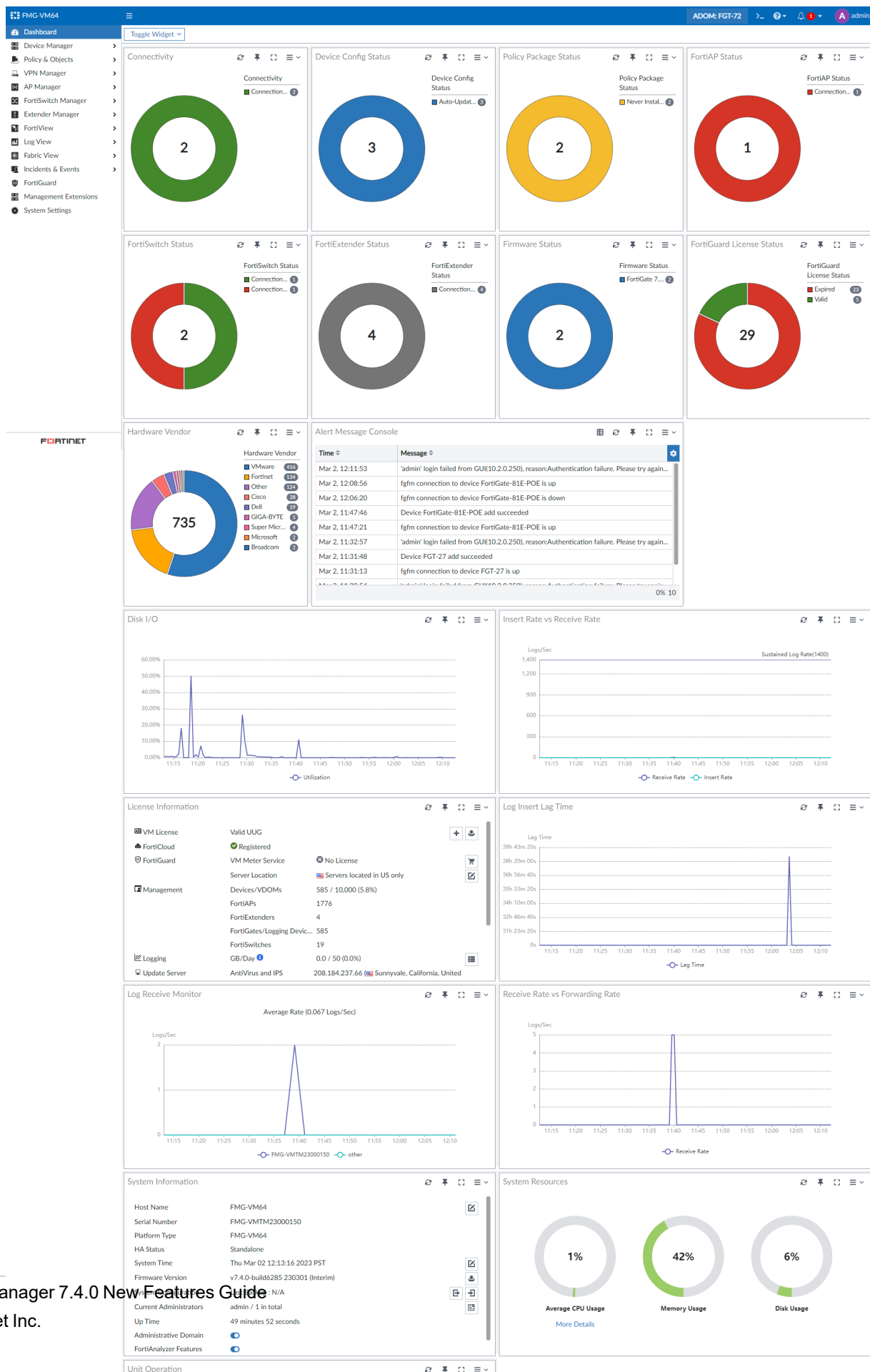
The FortiManager GUI now uses a new landing page called *Dashboard*. By default, the dashboard is displayed. You can access other pages, such as *Device Manager*, from the left-pane navigation.

The following new feature topic includes examples of some of the changes to the GUI introduced in FortiManager 7.4.0.

- [Dashboard on page 111](#)
- [Policy & Objects on page 113](#)
- [AP Manager on page 114](#)
- [Management Extensions on page 115](#)
- [System Settings on page 116](#)

Dashboard

- The *Dashboard* includes widgets, such as *Policy Package Status* and *Firmware Status*. You can toggle which widgets display from the *Toggle Widget* dropdown.



Policy & Objects

- Policy Package configuration:

Enterprise_FortiManager

Dashboard

Device Manager

Policy & Objects

Policy Packages

Normalized Interface

Firewall Objects

Security Profiles

User & Authentication

Security Fabric

Advanced

VPN Manager

AP Manager

FortiSwitch Manager

Extender Manager

Fabric View

FortiGuard

Management Extensions

System Settings

ADOM: ADOM1

>

?

1

F

Search...

Create New

Edit

Delete

Section

Policy Block

Policy Lookup

Collapse All

View Mode

Search

Enterprise_First_Floor_r...

Firewall Policy

Firewall Virtual Wire Pair P...

Authentication Rules

IPv4 Multicast Policy

IPv4 Local In Policy

IPv6 Local In Policy

IPv4 DoS Policy

IPv6 DoS Policy

IPv4 Interface Policy

NAC Policy

Traffic Shaping Policy

ZTNA Rules

Installation Targets

CLI Configurations

Enterprise_Second_Floor

default

Policy Blocks (0)

#	Name	From	To	Source	Destination	Schedule	Se
1		port3	port1	all	all	always	A
2		port2	port1	all	all	always	A
3		port1	port2	all	all	always	A
4		port1	port3	all	all	always	A
5		port2	port3	all	all	always	A
6		port3	port2	all	all	always	A
7	FTS_policy	port5	port6	all	all	always	A
8	FST Client>Upstream	port5	port1	all	all	always	A

0% 16

Fortinet

- Object configuration:

Enterprise_FortiManager

Dashboard

Device Manager

Policy & Objects

Policy Packages

Normalized Interface

Firewall Objects

Security Profiles

User & Authentication

Security Fabric

Advanced

VPN Manager

AP Manager

FortiSwitch Manager

Extender Manager

Fabric View

FortiGuard

Management Extensions

System Settings

Addresses

Internet Service

Services

Schedules

Virtual IPs

IP Pools

Shaping Profile

ZTNA Server

ZTNA Tag

ADOM: ADOM1

>

?

1

F

+ Create New

Edit

Delete

More

View

Search...

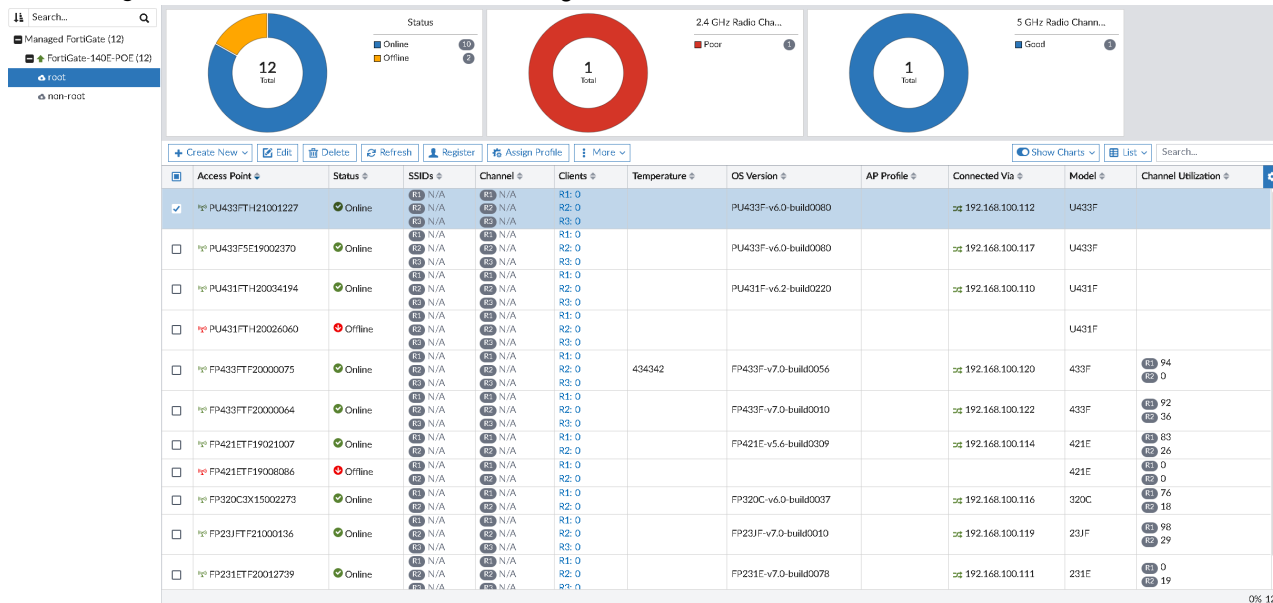
	Name	Type	Details	Interface	Comments	Created Time	Last
	Address 46						
	none	Address	IP/Netmask: 0.0.0.0/255.255.255.255	any		/ 2023-05-02 08:37:59	
	login.microsoftonline.com	Address	FQDN:login.microsoftonline.com	any		/ 2023-05-02 08:37:59	
	login.microsoft.com	Address	FQDN:login.microsoft.com	any		/ 2023-05-02 08:37:59	
	login.windows.net	Address	FQDN:login.windows.net	any		/ 2023-05-02 08:37:59	
	gmail.com	Address	FQDN:gmail.com	any		/ 2023-05-02 08:37:59	
	wildcard.google.com	Address	FQDN:*.google.com	any		/ 2023-05-02 08:37:59	
	wildcard.dropbox.com	Address	FQDN:*.dropbox.com	any		/ 2023-05-02 08:37:59	
	SSLVPN_TUNNEL_ADDR1	Address	IP Range: 192.168.1.100-192.168.1.200	any		/ 2023-05-02 08:37:59	
	all	Address	IP/Netmask: 0.0.0.0/0.0.0.0	any		/ 2023-05-02 08:37:59	
	FIREWALL_AUTH_PORTAL_ADDRESS	Address	IP/Netmask: 0.0.0.0/0.0.0.0	any		/ 2023-05-02 08:37:59	
	FABRIC_DEVICE	Address	IP/Netmask: 0.0.0.0/0.0.0.0	any	IPv4 addresses of Fabric Devi	/ 2023-05-02 08:37:59	
	metadata-server	Address	IP/Netmask: 192.168.1.100-192.168.1.200	any		/ 2023-05-02 08:37:59	
	RFC1918-10	Address	IP/Netmask: 10.0.0.0-10.255.255.255	any		/ 2023-05-02 08:37:59	
	RFC1918-172	Address	IP/Netmask: 172.16.0.0-172.31.255.255	any		/ 2023-05-02 08:37:59	
	RFC1918-192	Address	IP/Netmask: 192.168.0.0-192.168.255.255	any		/ 2023-05-02 08:37:59	

0%

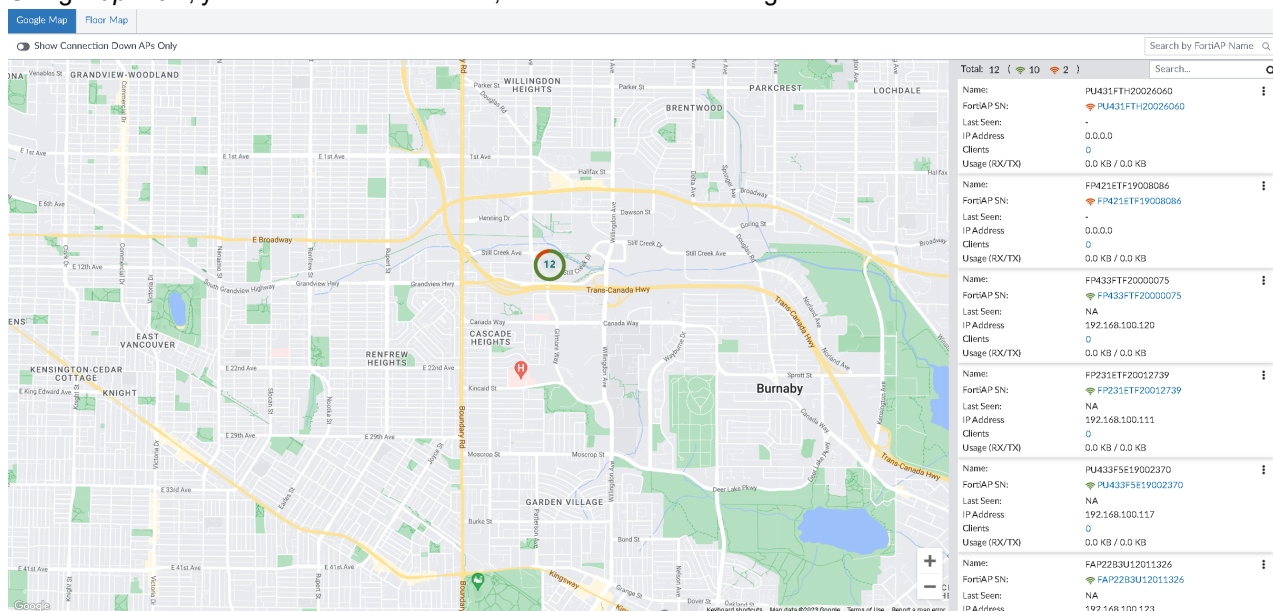
60

AP Manager

- Use *Managed FortiAPs* to view the status of managed FortiAP devices:



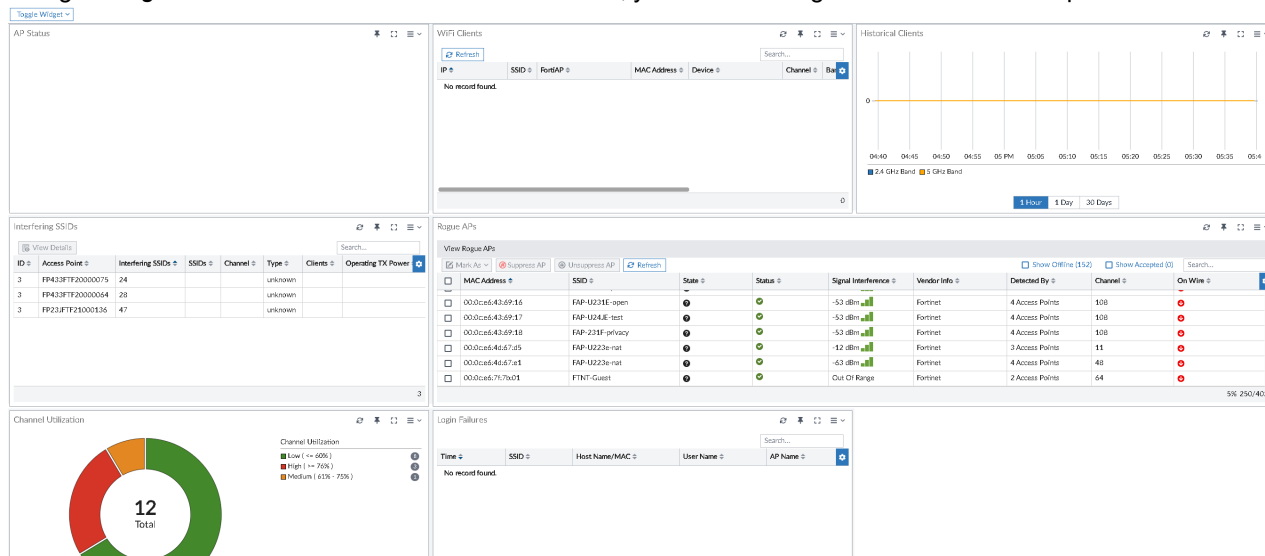
- Using *Map View*, you can check the location, info and status of managed FortiAP devices.



- Using *Operation Profiles*, *Connectivity Profiles*, and *Protection Profiles*, you can create different types of profiles and assign them to FortiAPs. Profile types, for example FortiAP profiles, are listed as tabs at the top of the page.

Name	Platform	Radio Mode	Bands	SSIDs	Comment
Corporate_Fortinet_Default		R1: Access Point R2: Access Point	R1: N/A R2: N/A	R1: All Tunnel Mode SSIDs R2: All Tunnel Mode SSIDs	Fortinet Recommended profile for Corporate
Guest_Fortinet_Default		R1: Access Point R2: Access Point	R1: N/A R2: N/A	R1: All Tunnel Mode SSIDs R2: All Tunnel Mode SSIDs	Fortinet Recommended profile for Guest
POS_Fortinet_Default		R1: Access Point R2: Access Point	R1: N/A R2: N/A	R1: All Tunnel Mode SSIDs R2: All Tunnel Mode SSIDs	Fortinet Recommended profile for POS

- Using *Managed FortiAPs* > *More* > *View Health Monitor*, you can see widgets related to the APs performance:



Management Extensions

- Updated Management Extensions layout:

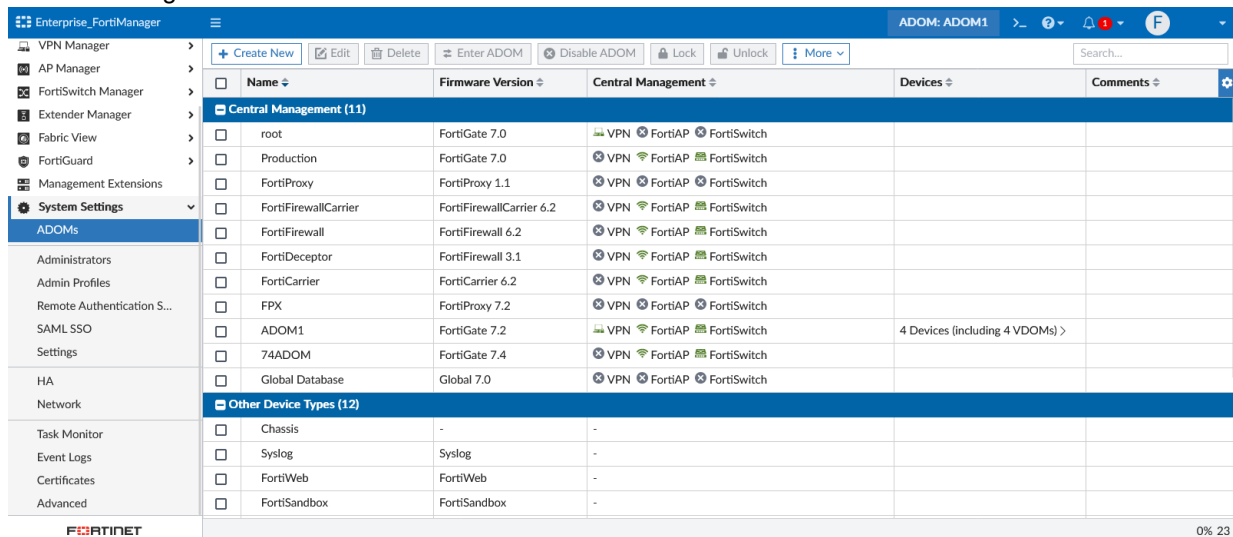
The updated Management Extensions layout features a grid of extension tiles, each representing a different management extension:

- FortiPortal
- FortiWLM
- FortiSigConverter
- FortiSOAR
- Policy Analyzer
- FortiAIOps
- Universal Connector

System Settings

System settings are available as tabs at the top of the system settings page.

- ADOMs settings:

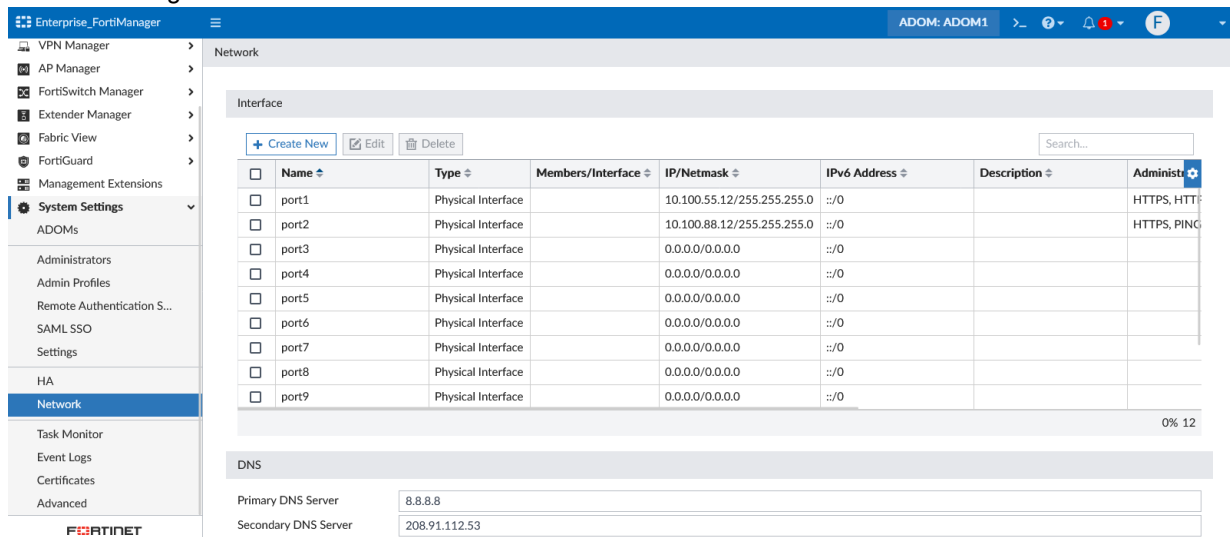


The screenshot shows the FortiManager System Settings page with the ADOMs tab selected. The left sidebar contains a navigation menu with options like VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, Fabric View, FortiGuard, Management Extensions, System Settings (selected), ADOMs, Administrators, Admin Profiles, Remote Authentication S..., SAML SSO, Settings, HA, Network, Task Monitor, Event Logs, Certificates, and Advanced. The main content area displays a table of ADOMs and other device types.

Name	Firmware Version	Central Management	Devices	Comments
Central Management (11)				
<input type="checkbox"/> root	FortiGate 7.0	VPN FortiAP FortiSwitch		
<input type="checkbox"/> Production	FortiGate 7.0	VPN FortiAP FortiSwitch		
<input type="checkbox"/> FortiProxy	FortiProxy 1.1	VPN FortiAP FortiSwitch		
<input type="checkbox"/> FortiFirewallCarrier	FortiFirewallCarrier 6.2	VPN FortiAP FortiSwitch		
<input type="checkbox"/> FortiFirewall	FortiFirewall 6.2	VPN FortiAP FortiSwitch		
<input type="checkbox"/> FortiDeceptor	FortiFirewall 3.1	VPN FortiAP FortiSwitch		
<input type="checkbox"/> FortiCarrier	FortiCarrier 6.2	VPN FortiAP FortiSwitch		
<input type="checkbox"/> FPX	FortiProxy 7.2	VPN FortiAP FortiSwitch		
<input type="checkbox"/> ADOM1	FortiGate 7.2	VPN FortiAP FortiSwitch	4 Devices (including 4 VDOMs) >	
<input type="checkbox"/> 74ADOM	FortiGate 7.4	VPN FortiAP FortiSwitch		
<input type="checkbox"/> Global Database	Global 7.0	VPN FortiAP FortiSwitch		
Other Device Types (12)				
<input type="checkbox"/> Chassis	-	-		
<input type="checkbox"/> Syslog	Syslog	-		
<input type="checkbox"/> FortiWeb	FortiWeb	-		
<input type="checkbox"/> FortiSandbox	FortiSandbox	-		

0% 23

- Network settings:



The screenshot shows the FortiManager System Settings page with the Network tab selected. The left sidebar is the same as the previous screenshot. The main content area displays the Network settings, including a table of interfaces and DNS settings.

Name	Type	Members/Interface	IP/Netmask	IPv6 Address	Description	Adminis
<input type="checkbox"/> port1	Physical Interface		10.100.55.12/255.255.255.0	::/0		HTTPS, HTTP
<input type="checkbox"/> port2	Physical Interface		10.100.88.12/255.255.255.0	::/0		HTTPS, PING
<input type="checkbox"/> port3	Physical Interface		0.0.0.0/0.0.0.0	::/0		
<input type="checkbox"/> port4	Physical Interface		0.0.0.0/0.0.0.0	::/0		
<input type="checkbox"/> port5	Physical Interface		0.0.0.0/0.0.0.0	::/0		
<input type="checkbox"/> port6	Physical Interface		0.0.0.0/0.0.0.0	::/0		
<input type="checkbox"/> port7	Physical Interface		0.0.0.0/0.0.0.0	::/0		
<input type="checkbox"/> port8	Physical Interface		0.0.0.0/0.0.0.0	::/0		
<input type="checkbox"/> port9	Physical Interface		0.0.0.0/0.0.0.0	::/0		

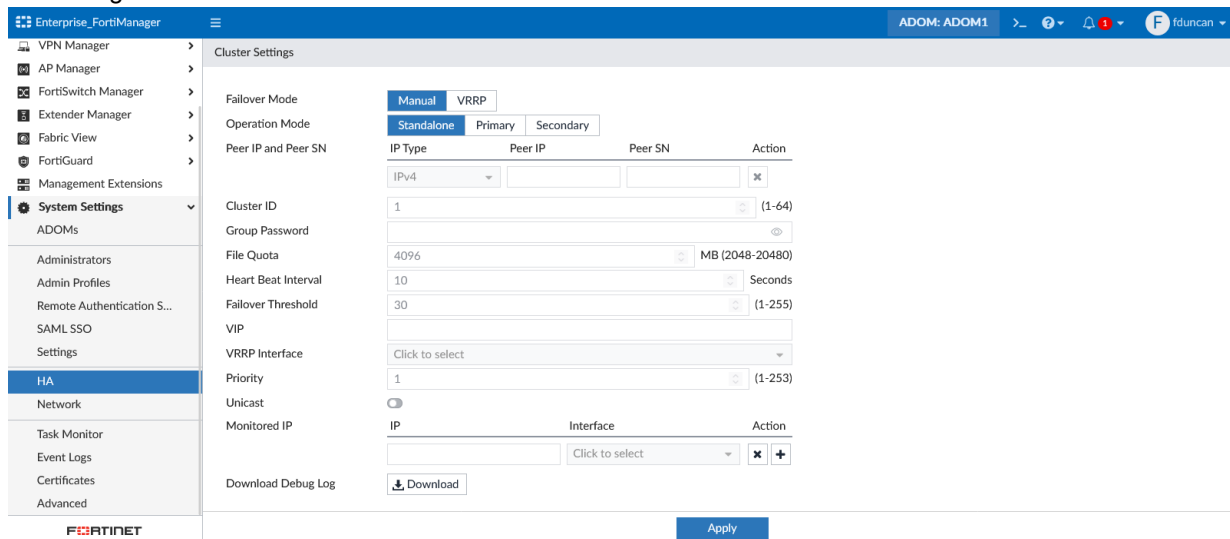
0% 12

DNS

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 208.91.112.53

- HA settings:



The screenshot shows the FortiManager web interface for HA settings. The left sidebar contains a menu with 'System Settings' expanded, showing 'HA' as the selected option. The main content area is titled 'Cluster Settings' and contains various configuration fields. At the top, there are tabs for 'Manual' and 'VRRP'. Below these are tabs for 'Standalone', 'Primary', and 'Secondary'. The 'Peer IP and Peer SN' section has a table with columns for IP Type, Peer IP, Peer SN, and Action. The 'Cluster ID' is set to 1. The 'Group Password' is empty. The 'File Quota' is set to 4096 MB. The 'Heart Beat Interval' is 10 seconds. The 'Failover Threshold' is 30. The 'VIP' is empty. The 'VRRP Interface' is set to 'Click to select'. The 'Priority' is 1. The 'Unicast' checkbox is checked. The 'Monitored IP' section has a table with columns for IP, Interface, and Action. At the bottom, there is a 'Download Debug Log' button and an 'Apply' button.

Enterprise_FortiManager

ADOM: ADOM1

Cluster Settings

Failover Mode: Manual VRRP

Operation Mode: Standalone Primary Secondary

Peer IP and Peer SN

IP Type	Peer IP	Peer SN	Action
IPv4			

Cluster ID: 1 (1-64)

Group Password:

File Quota: 4096 MB (2048-20480)

Heart Beat Interval: 10 Seconds

Failover Threshold: 30 (1-255)

VIP:

VRRP Interface: Click to select

Priority: 1 (1-253)

Unicast: ☒

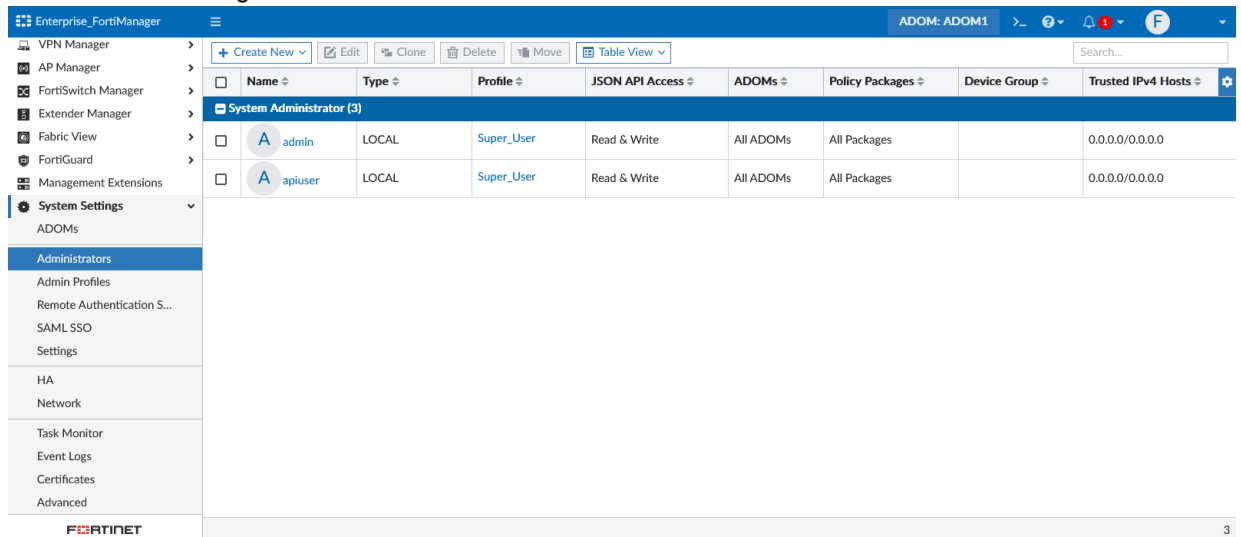
Monitored IP

IP	Interface	Action
	Click to select	

Download Debug Log: Download

Apply

- Administrators settings:



The screenshot shows the FortiManager web interface for Administrators settings. The left sidebar contains a menu with 'System Settings' expanded, showing 'Administrators' as the selected option. The main content area shows a table of administrators. At the top, there are buttons for '+ Create New', 'Edit', 'Clone', 'Delete', 'Move', and 'Table View'. A search bar is also present. The table has columns for Name, Type, Profile, JSON API Access, ADOMs, Policy Packages, Device Group, and Trusted IPv4 Hosts. There are two administrators listed: 'admin' and 'apiuser'.

Enterprise_FortiManager

ADOM: ADOM1

+ Create New Edit Clone Delete Move Table View

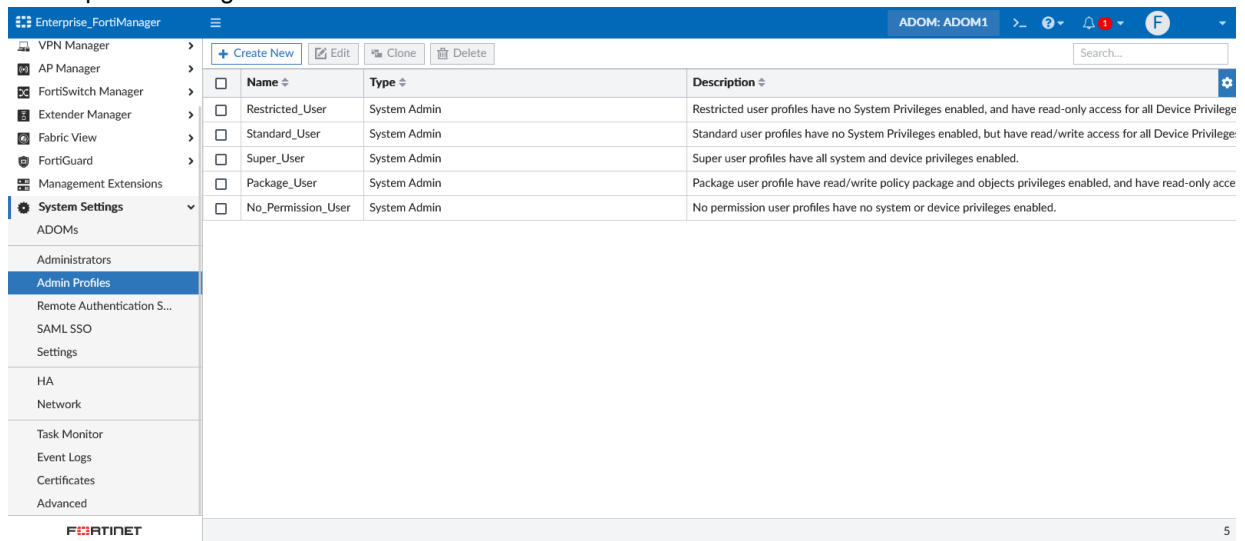
Search...

Name	Type	Profile	JSON API Access	ADOMs	Policy Packages	Device Group	Trusted IPv4 Hosts
admin	LOCAL	Super_User	Read & Write	All ADOMs	All Packages		0.0.0.0/0.0.0.0
apiuser	LOCAL	Super_User	Read & Write	All ADOMs	All Packages		0.0.0.0/0.0.0.0

System Administrator (3)

3

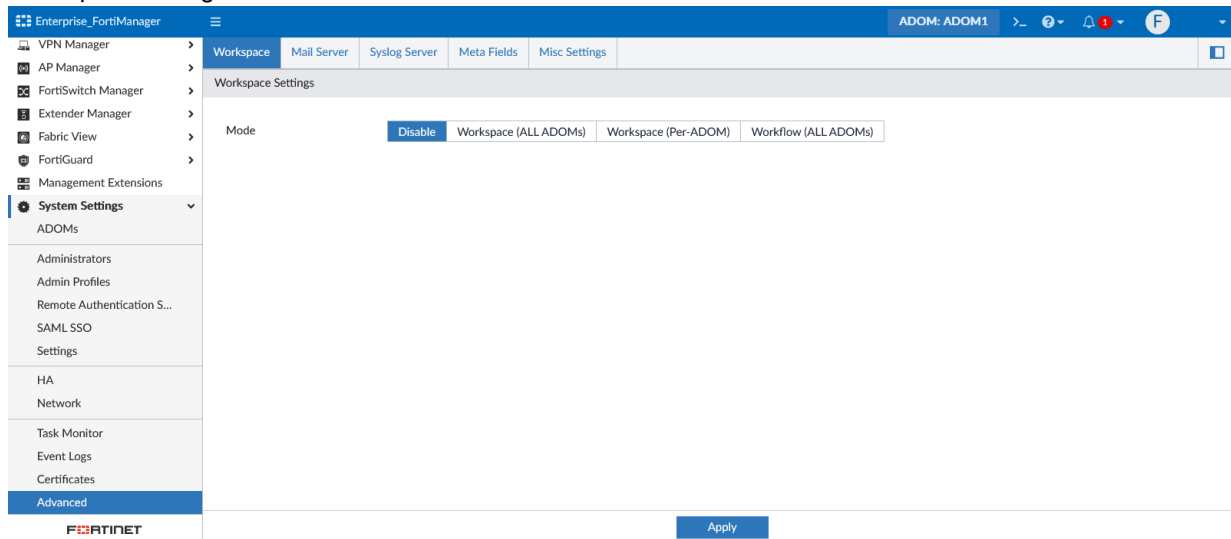
- Admin profile settings:



The screenshot shows the FortiManager web interface for 'Enterprise_FortiManager'. The left sidebar lists various management sections, with 'System Settings' expanded to show 'Admin Profiles'. The main content area displays a table of admin profiles. At the top, there are buttons for 'Create New', 'Edit', 'Clone', and 'Delete', along with a search bar. The table has columns for 'Name', 'Type', and 'Description'. The 'Name' column includes checkboxes for each profile.

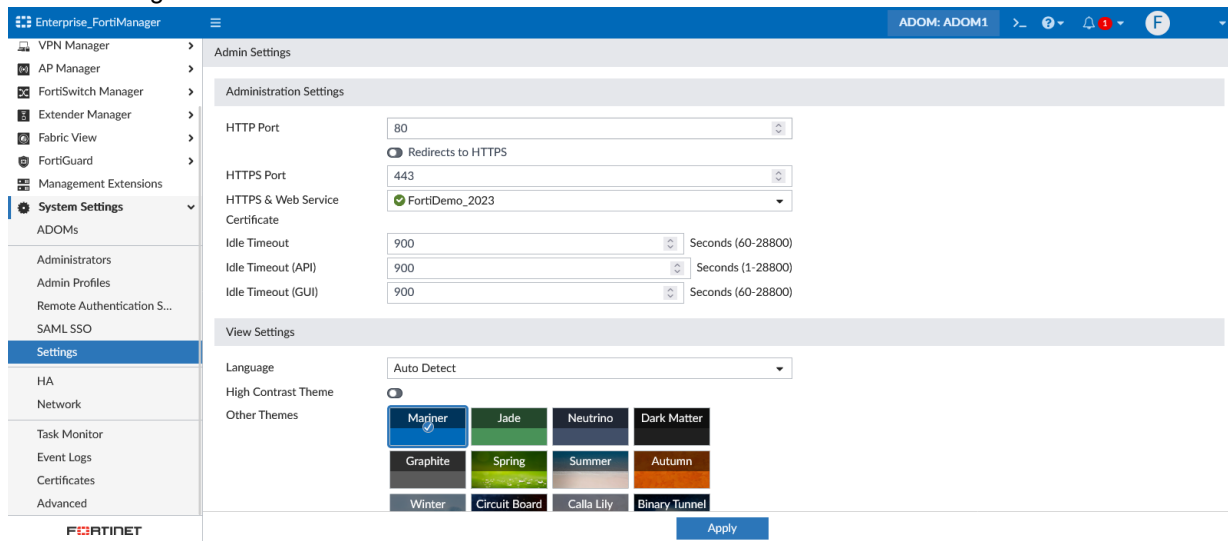
<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Restricted_User	System Admin	Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privilege
<input type="checkbox"/>	Standard_User	System Admin	Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privilege
<input type="checkbox"/>	Super_User	System Admin	Super user profiles have all system and device privileges enabled.
<input type="checkbox"/>	Package_User	System Admin	Package user profile have read/write policy package and objects privileges enabled, and have read-only acce
<input type="checkbox"/>	No_Permission_User	System Admin	No permission user profiles have no system or device privileges enabled.

- Workspace settings:



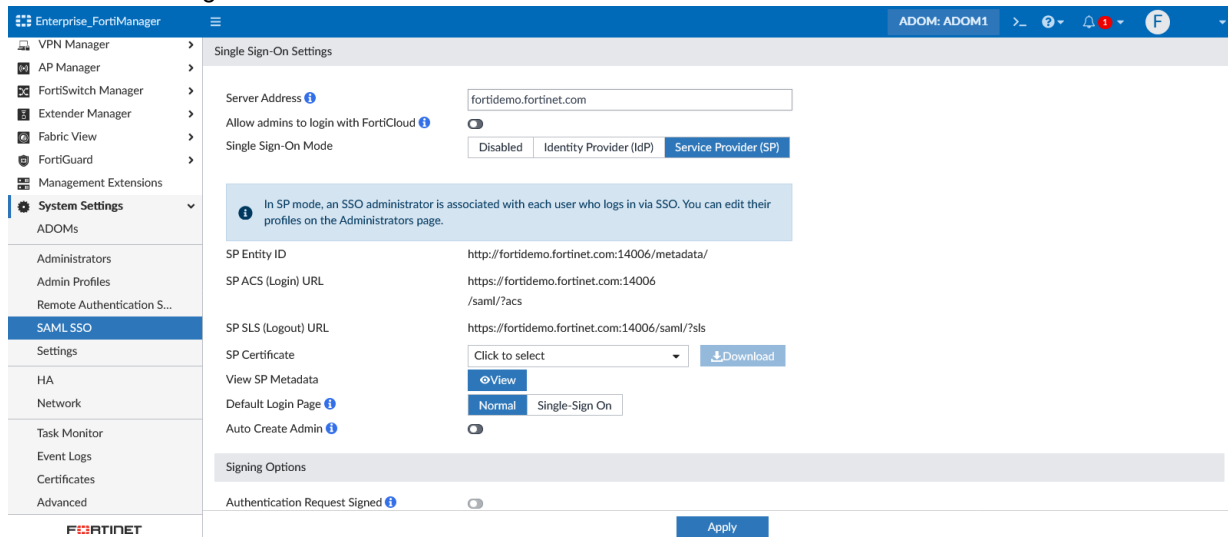
The screenshot shows the FortiManager web interface for 'Enterprise_FortiManager'. The left sidebar is the same as the previous screenshot, with 'System Settings' expanded to 'Advanced'. The main content area is titled 'Workspace Settings' and has tabs for 'Workspace', 'Mail Server', 'Syslog Server', 'Meta Fields', and 'Misc Settings'. The 'Workspace' tab is active, showing a 'Mode' section with four buttons: 'Disable', 'Workspace (ALL ADOMs)', 'Workspace (Per-ADOM)', and 'Workflow (ALL ADOMs)'. An 'Apply' button is at the bottom right.

- Admin Settings:



The screenshot shows the FortiManager web interface. The left sidebar contains a menu with categories like VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, Fabric View, FortiGuard, Management Extensions, System Settings (selected), ADOMs, Administrators, Admin Profiles, Remote Authentication S..., SAML SSO, Settings (highlighted), HA, Network, Task Monitor, Event Logs, Certificates, and Advanced. The main content area is titled 'Admin Settings' and 'Administration Settings'. It includes fields for HTTP Port (80), HTTPS Port (443), and HTTP & Web Service Certificate (FortiDemo_2023). There are also fields for Idle Timeout (900 seconds) for API and GUI. Below these are 'View Settings' for Language (Auto Detect) and High Contrast Theme (disabled). A grid of theme thumbnails is shown, with 'Mariner' selected. An 'Apply' button is at the bottom right.

- SAML SSO settings:



The screenshot shows the FortiManager web interface for SAML SSO settings. The left sidebar is the same as the previous screenshot, with 'SAML SSO' selected under 'System Settings'. The main content area is titled 'Single Sign-On Settings'. It includes a 'Server Address' field (fortidemo.fortinet.com), a toggle for 'Allow admins to login with FortiCloud', and a 'Single Sign-On Mode' section with buttons for 'Disabled', 'Identity Provider (IdP)', and 'Service Provider (SP)'. A blue information box states: 'In SP mode, an SSO administrator is associated with each user who logs in via SSO. You can edit their profiles on the Administrators page.' Below this are fields for SP Entity ID, SP ACS (Login) URL, SP SLS (Logout) URL, and SP Certificate (with a 'Click to select' dropdown and a 'Download' button). There are also buttons for 'View SP Metadata' (Normal, Single-Sign On) and 'Auto Create Admin'. A 'Signing Options' section at the bottom has a toggle for 'Authentication Request Signed'. An 'Apply' button is at the bottom right.

• Certificate settings:

Enterprise_FortiManager

ADOM: ADOM1

Search...

Certificate Name	Subject	Status	Issuer	Expiration Date
Local CA Certificate (3)				
<input type="checkbox"/> Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	OK	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	2056-05-27 20:27:39 GMT
<input type="checkbox"/> Fortinet_CA2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	OK	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	2056-01-19 22:34:39 GMT
<input type="checkbox"/> Fortinet_SUBCA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	OK	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	2056-05-27 20:48:33 GMT
Local Certificate (3)				
<input type="checkbox"/> FortiDemo_2023	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", ...	OK	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2...	2023-09-18 23:59:59 GMT
<input type="checkbox"/> Fortinet_Local	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = F...	OK	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	2038-01-19 03:14:07 GMT
<input type="checkbox"/> Fortinet_Local2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = F...	OK	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	2038-01-19 03:14:07 GMT
CRL (0)				
Remote CA Certificate (2)				
<input type="checkbox"/> Remote_Cert_1	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = F...	OK	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	2056-01-19 03:14:07 GMT
<input type="checkbox"/> Remote_Cert_2	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", ...	OK	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = Di...	2021-09-15 12:00:00 GMT

8

• Event Log settings:

Enterprise_FortiManager

ADOM: ADOM1

Add Filter

Last 1 Hour

Download Raw Log Historical Log

#	Date Time	Level	User	Sub Type	Description	Operation
1	2023-05-09 13:24:50	information	__docker_fortiportal-JSON(169.254.255.50)	System manager event	User login/logout successful	logout
2	2023-05-09 13:24:20	information	update_manager	FortiGuard service event	Package update response from FortiGuard server received	Update Response
3	2023-05-09 13:20:32	information	__docker_fortiportal-JSON(169.254.255.50)	System manager event	User login/logout successful	logout
4	2023-05-09 13:20:32	information	__docker_fortiportal-JSON(169.254.255.50)	System manager event	User login/logout successful	login
5	2023-05-09 13:19:42	information	__docker_fortiportal-JSON(169.254.255.50)	System manager event	User login/logout successful	login
6	2023-05-09 13:15:32	information	__docker_fortiportal-JSON(169.254.255.50)	System manager event	User login/logout successful	logout
7	2023-05-09 13:15:32	information	__docker_fortiportal-JSON(169.254.255.50)	System manager event	User login/logout successful	login
8	2023-05-09 13:14:50	information	__docker_fortiportal-JSON(169.254.255.50)	System manager event	User login/logout successful	logout
9	2023-05-09 13:14:09	information	update_manager	FortiGuard service event	Package update response from FortiGuard server received	Update Response
10	2023-05-09 13:10:48	information		Device manager event	Device Manager dvm log at information level	Switch to new ADOM
11	2023-05-09 13:10:32	information	__docker_fortiportal-JSON(169.254.255.50)	System manager event	User login/logout successful	logout
12	2023-05-09 13:10:32	information	__docker_fortiportal-JSON(169.254.255.50)	System manager event	User login/logout successful	login

50 /Page 1 2 3 4 5 295

• Misc settings:

Enterprise_FortiManager

ADOM: ADOM1

Workspace Mail Server Syslog Server Meta Fields Misc Settings

Advanced Settings

Offline Mode ☒ Normal ☐ Advanced

ADOM Mode ☒ Normal ☐ Advanced

Download WSDL File ☒ Legacy Operations ☐ System Commands

☒ CLI Configuration ☐ Device Manager Commands

☐ Device Manager Database ☐ Task Database

☐ Security Console ☐ Policy Package

☐ System Template ☐ ADOM Objects

☐ CDB Auxiliary

Download

Chassis Management

Configuration Changes Received from FortiGate ☒ Automatically accept ☐ Prompt Administrator to accept

Task List Size 2000

Verify Installation ☒

Allow Install Interface Policy Only ☒

Display Policy & Objects in Classic Dual Pane ☒

Display Device/Group tree view in Device Manager ☒

Apply

Fabric and External connector pages have been reorganized for an enhanced user experience

Fabric and External connector pages have been reorganized for an enhanced user experience, similar to the experience in FortiOS.

To view and configure connectors in Fabric View:

1. Go to *Fabric View*. The *Fabric Connectors* and *External Connectors* pages are available in the tree menu under *Fabric View*.

The following connector types have been moved into the *External Connectors* menu.

- Public SDN
- Private SDN
- Threat Feeds

- Endpoint/Identity

Dashboard

- Device Manager
- Policy & Objects
- VPN Manager
- AP Manager
- FortiSwitch Manager
- Extender Manager
- Fabric View**
 - Physical Topology
 - Logical Topology
 - Security Rating
 - Fabric Connectors
 - External Connectors**
 - Cloud Orchestration
 - FortiGuard
 - Management Extensions
 - System Settings

Create New Fabric Connector - Select Connector Type (1/2)

Please choose a connector type

Public SDN (6)

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI)
- AliCloud
- IBM Cloud

Private SDN (8)

- Kubernetes
- VMware ESXi
- VMware NSX-V
- OpenStack (Horizon)
- Application Centric Infrastructure (ACI)
- Nuage Virtualized Service Platform
- Nutanix
- SAP

Threat Feeds (4)

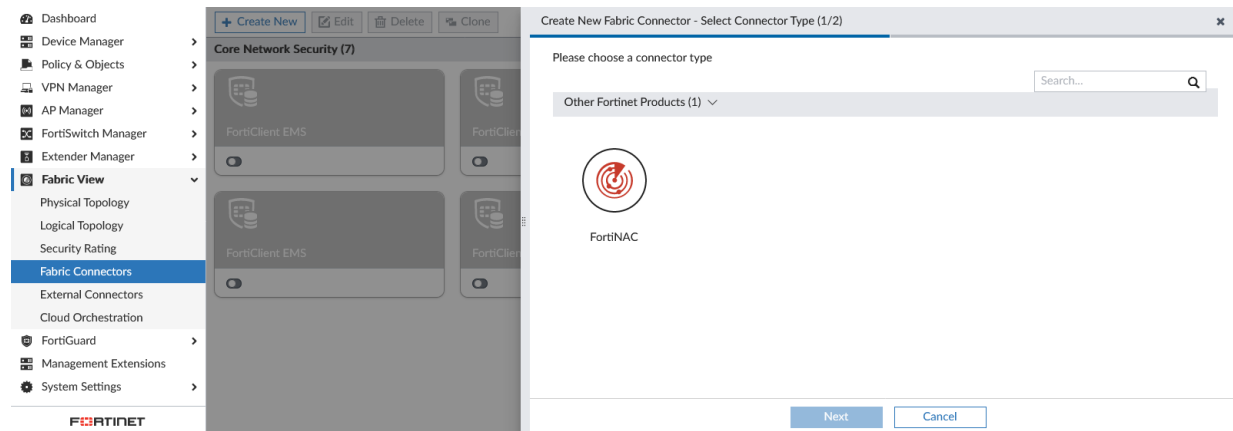
- FortiGuard Category Threat Feed
- IP Address Threat Feed
- Domain Name Threat Feed
- Malware Hash Threat Feed

Endpoint/Identity (10)

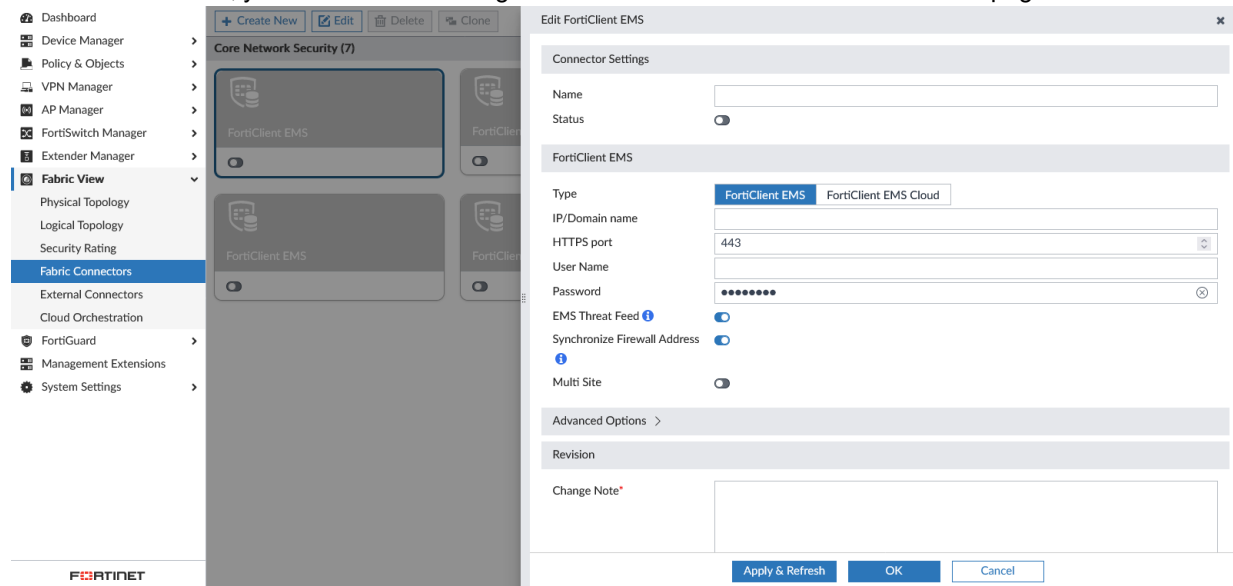
- Poll Active Directory Server
- Fortinet Single Sign-On Agent
- RADIUS Single Sign-On Agent
- User pxGrid
- User ClearPass
- VMware NSX-T
- VMware vCenter
- Symantec Endpoint Protection
- Exchange Server
- JSON API Connector

Next Cancel

The *FortiClient EMS* and *FortiNAC* connectors have been moved into the *Fabric Connectors* menu.



- Click *Create New* to create a new connector while in the *Fabric Connectors* or *External Connectors* view. For *FortiClient EMS*, you can edit the existing EMS connectors on the *Fabric Connectors* page.



To view and configure connectors in Policy & Objects:

- Go to *Policy & Objects > Security Fabric*.
The *Fabric Connectors*, *SDN Connectors*, and *Endpoint/Identity* menus are available as tabs.

- Public and Private SDN connector types are included in the *SDN Connectors* tab.

The screenshot shows the FortiManager interface with the 'SDN Connectors' tab selected. The left sidebar shows the navigation menu with 'Policy & Objects' expanded. The main panel shows the 'SDN Connectors' tab with a table listing connectors. A dropdown menu is open, showing options like 'Public SDN Connector', 'Private SDN Connector', and 'AWS_VPC'.

Type	IP/Port	Created Time	Last Modified	Revision History
Public SDN Connector				
Private SDN Connector				
AWS_VPC	Amazon Web Services (AWS)	fduncan / 2023-05-02 08:47:05		

- Endpoint and identity connectors are included in the *Endpoint/Identity* tab.

The screenshot shows the FortiManager interface with the 'Endpoint/Identity' tab selected. The left sidebar shows the navigation menu with 'Policy & Objects' expanded. The main panel shows the 'Endpoint/Identity' tab with a table listing connectors. A dropdown menu is open, showing options like 'Poll Active Directory Server', 'Fortinet Single Sign-On Agent', 'RADIUS Single Sign-On Agent', 'pxGrid Connector', 'ClearPass Connector', 'NSX-T Connector', 'Flex-VM Connector', 'vCenter Connector', 'Symantec Endpoint Protection', 'Exchange Server Connector', and 'JSON API Connector'.

Details	Created Time	Last Modified	Revision History
Poll Active Directory Server			
Fortinet Single Sign-On Agent			
RADIUS Single Sign-On Agent			
pxGrid Connector			
ClearPass Connector			
NSX-T Connector			
Flex-VM Connector			
vCenter Connector			
Symantec Endpoint Protection			
Exchange Server Connector			
JSON API Connector			

- FortiClient EMS and FortiNAC connectors are included in the *Fabric Connectors* tab.

The screenshot shows the FortiManager interface with the 'Fabric Connectors' tab selected. The left sidebar shows the navigation menu with 'Policy & Objects' expanded. The main panel shows the 'Fabric Connectors' tab with a table listing connectors. A dropdown menu is open, showing options like 'FortiClient EMS' and 'FortiNAC'.

Name/ID	Type	Details	Created Time	Last Modified	Revision History
FortiClient EMS					
1	FortiClient EMS	Server N/A:443			
2	FortiClient EMS	Server N/A:443			
3	FortiClient EMS	Server N/A:443			
4	FortiClient EMS	Server N/A:443			
5	FortiClient EMS	Server N/A:443			
6	FortiClient EMS	Server N/A:443			
7	FortiClient EMS	Server N/A:443			
FortiNAC					

2. To configure FortiClient EMS connectors, navigate to *Policy & Objects > Security Fabric > Fabric Connectors*, and select an existing EMS connector to edit and make changes to it.

The screenshot shows the 'Edit FortiClient EMS' configuration window. The left pane displays a table of existing connectors:

Name/ID	Type
1	FortiClient EMS
2	FortiClient EMS
3	FortiClient EMS
4	FortiClient EMS
5	FortiClient EMS
6	FortiClient EMS
7	FortiClient EMS

The right pane shows the configuration for connector 1:

- Connector Settings:** Name (empty), Status (disabled).
- FortiClient EMS:** Type (FortiClient EMS), IP/Domain name (empty), HTTPS port (443), User Name (empty), Password (masked), EMS Threat Feed (enabled), Synchronize Firewall Address (enabled), Multi Site (disabled).
- Advanced Options:** (collapsed)

3. To configure FortiNAC connectors, navigate to *Policy & Objects > Security Fabric > Fabric Connectors* and click *Create New*.

The screenshot shows the 'Create New FortiNAC' configuration window. The left pane displays a message: "No record found." The right pane shows the configuration details for a new FortiNAC connector:

- Name:** (empty, required field)
- Type:** FortiNAC
- FSSO Agent:** IP/Name, Password, Port, Action
- User Group Source:** Collector Agent, Via FortiGate, Local
- User Groups (0):** (empty)
- SSL:** (disabled)
- Advanced Options:** (collapsed)
- Per-Device Mapping:** (collapsed)
- Revision:** (empty)
- Change Note:** (empty)

FortiManager connector relay to AWS will proxy all individual FortiGate requests



This information is also available in the FortiManager 7.4 Administration Guide:

- [Using FortiManager as an SDN proxy for AWS connectors](#)

FortiManager connector relay to AWS will proxy all individual FortiGate requests.

This feature can only be configured using the CLI.

To configure the FortiManager connector relay to AWS:

1. In the FortiGate CLI, create the proxy object:

```
config system sdn-proxy <---- new object
    edit <sdn-proxy name>
        set type fortimanager
        set server <server address>
        set username <username">
        set password <password>
    next
end
```

2. In the FortiGate CLI, configure the SDN connector to use the proxy.

```
config system sdn-connector
    edit "aws1"
        set proxy <sdn-proxy name> <---- new property
        set use-metadata-iam disable
        set access-key <access>
        set secret-key <secret>
        set region "us-west-2"
    next
end
```

3. On the FortiManager, you can manage the SDN proxy daemon with the following commands in the CLI:

- The *sdnproxy* daemon is able to restart by using the `diagnose test application sdnproxyd <xx>` command where *xx* is the level of debug.
- The *sdnproxy* daemon shows debug logs using the `diagnose debug application sdnproxy <xx>` command where *xx* is the level of debug.

FortiManager key areas have been reorganized to enhance user experience

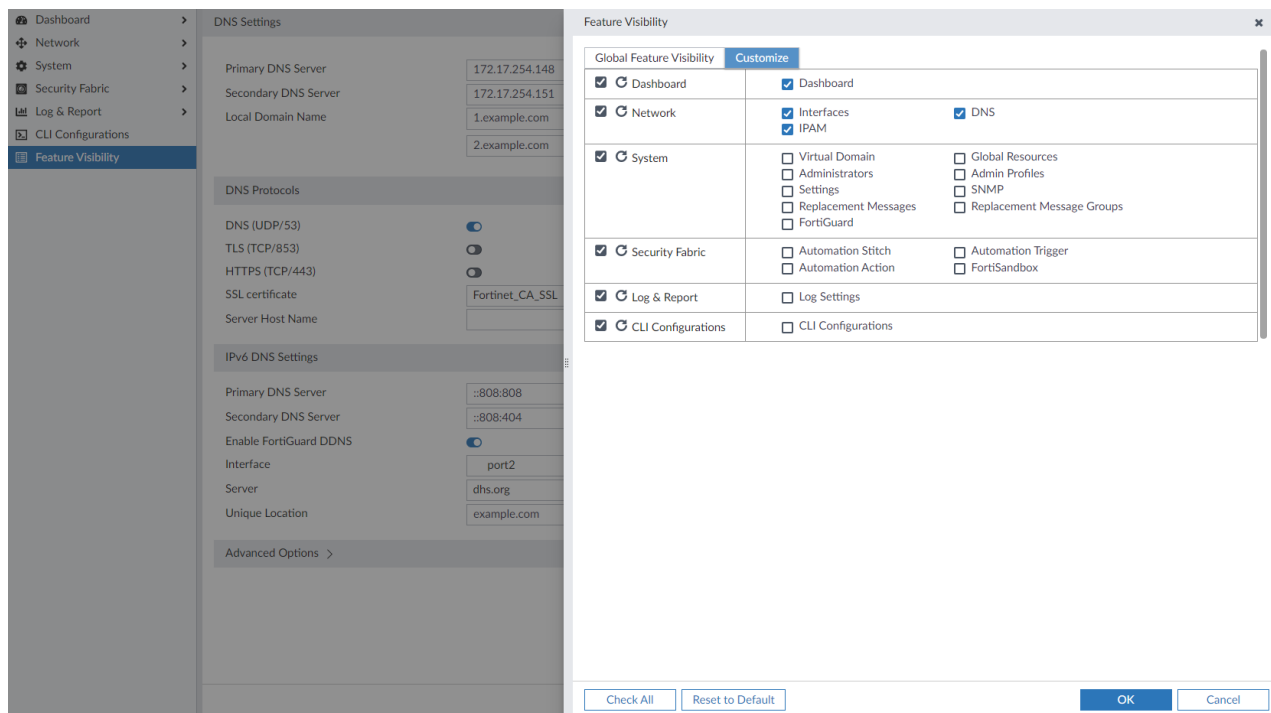
FortiManager key areas have been reorganized to enhance user experience, similar to FortiOS.

This topic includes the following sections:

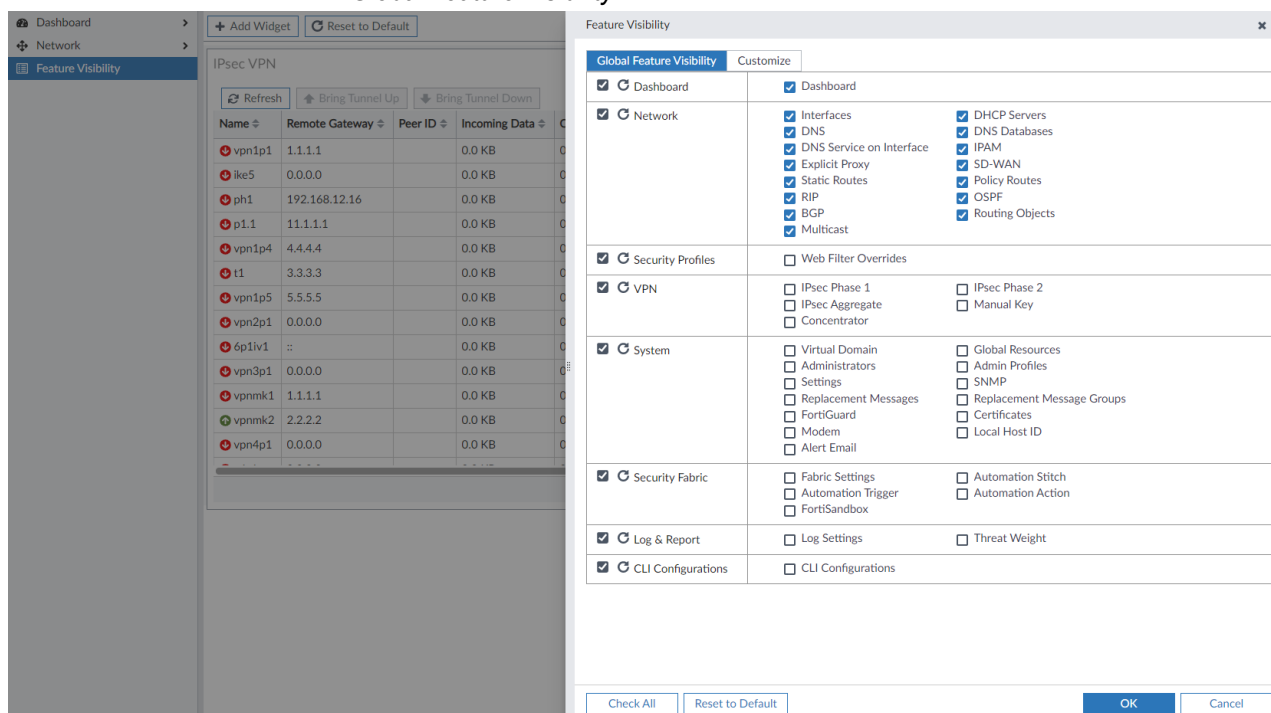
- [Device Manager on page 126](#)
- [Firewall Objects on page 134](#)
- [Fabric Connector on page 135](#)
- [Firewall Policies on page 136](#)
- [FortiAP Manager on page 136](#)
- [FortiSwitch Manager on page 139](#)

Device Manager

- In the *Device Manager* device database, you can use *Feature Visibility* to enable network related features under the *Network* tree in the VDOM level.

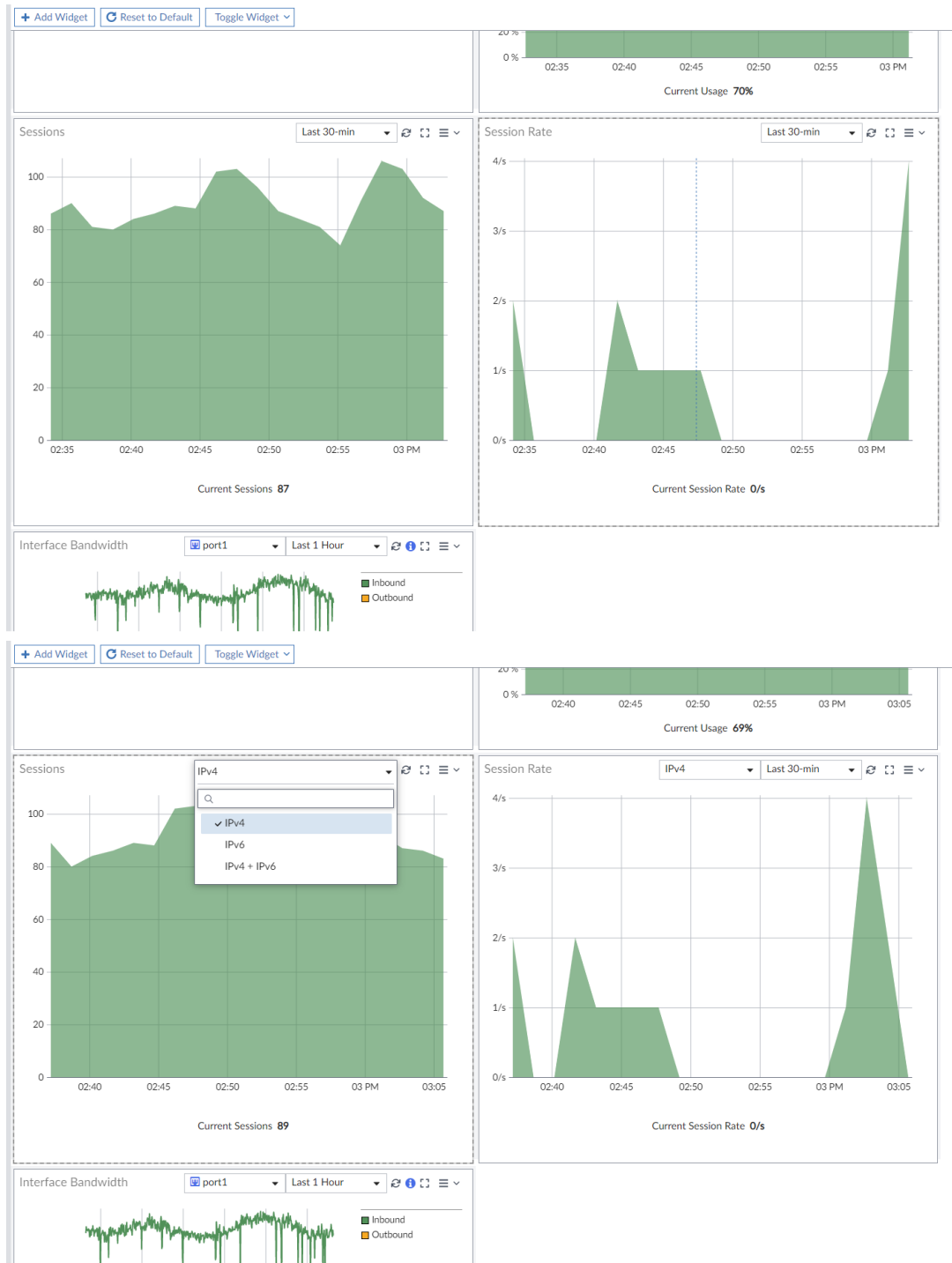


- Enable network features in the *Global Feature Visibility* menu.



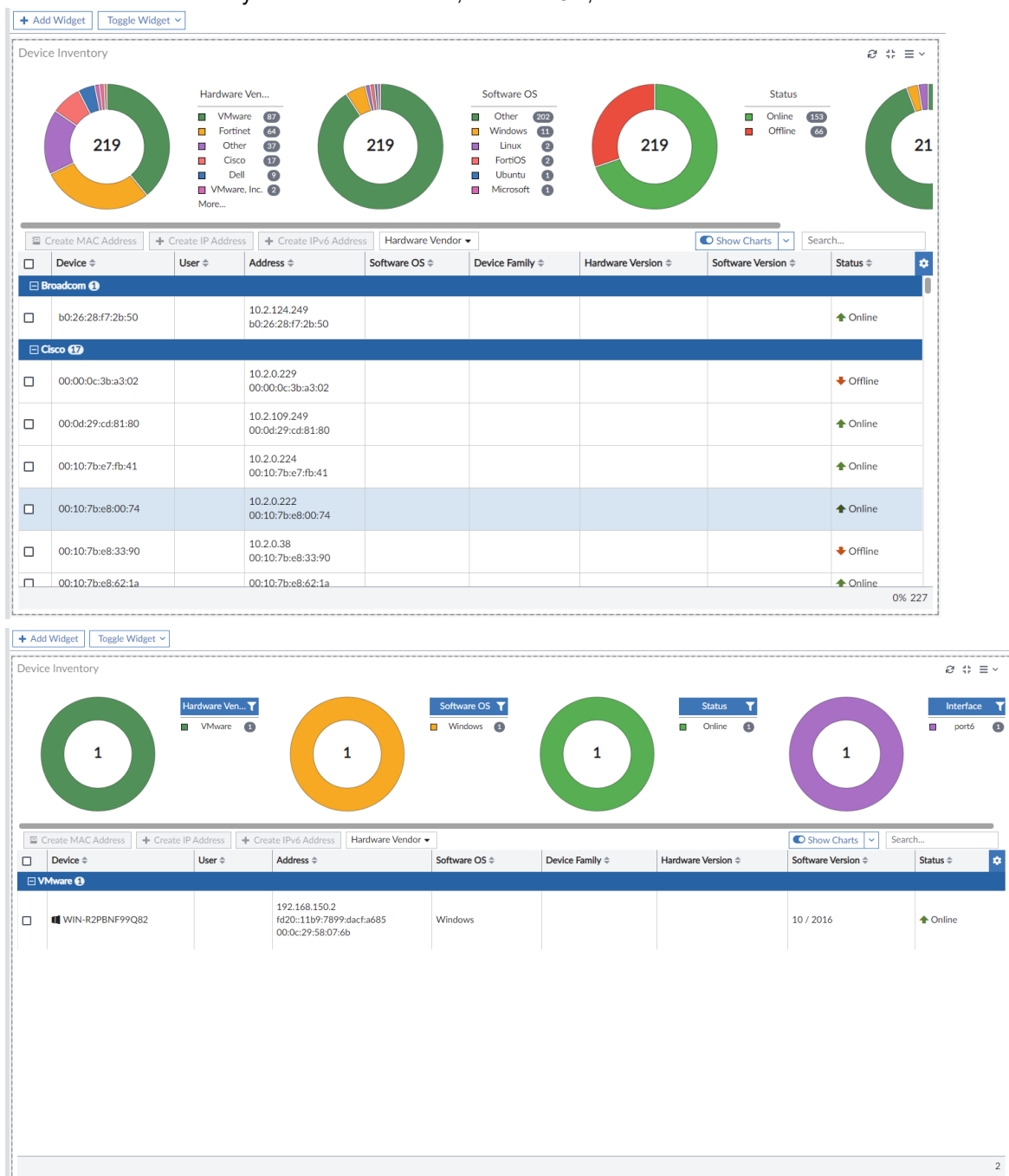
- Network related device configuration features are moved under the *Network* tree group. The following features have been moved from the *Router* and *System* menu to the new *Network* menu.
 - Interfaces
 - DHCP Servers
 - SD-WAN
 - DNS (Global tree feature)

- DNS Database
- DNS Service on Interface
- IPAM (Global tree feature)
- Explicit Proxy
- Static Routes
- Policy Routes
- RIP
- OSPF
- BGP
- Routing Objects
- Multicast
- The following device dashboard widgets are new or improved:
 - *Session* and *Session Rate*:
 - Changed from a line chart to an area chart.
 - Displays a dropdown list when IPv6 is enabled on FortiGate (options include: IPV4, IPV6, and IPV4 + IPV6), and displays the relevant chart based on the selected option.

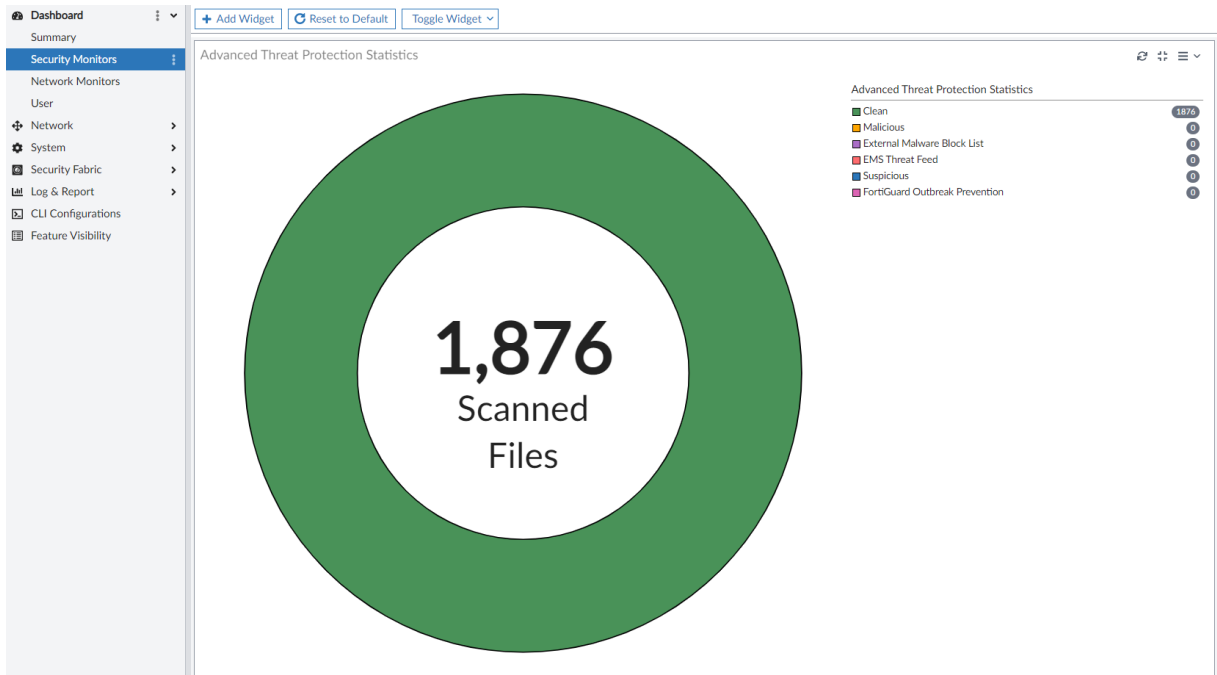


- **Device Inventory:**
 - The widget has added donut charts.
 - You can group and display the results by the hardware vendor or software OS.

- You can filter the result by the hardware vendor, software OS, status and interface.

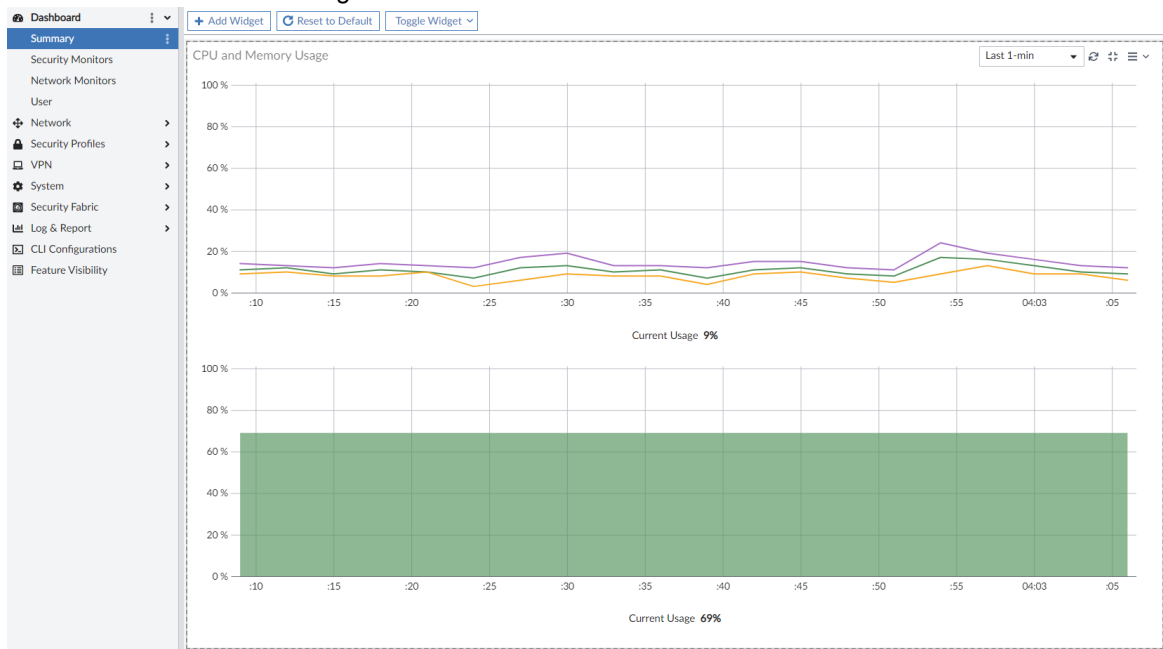


- **Advanced Host Scan:**

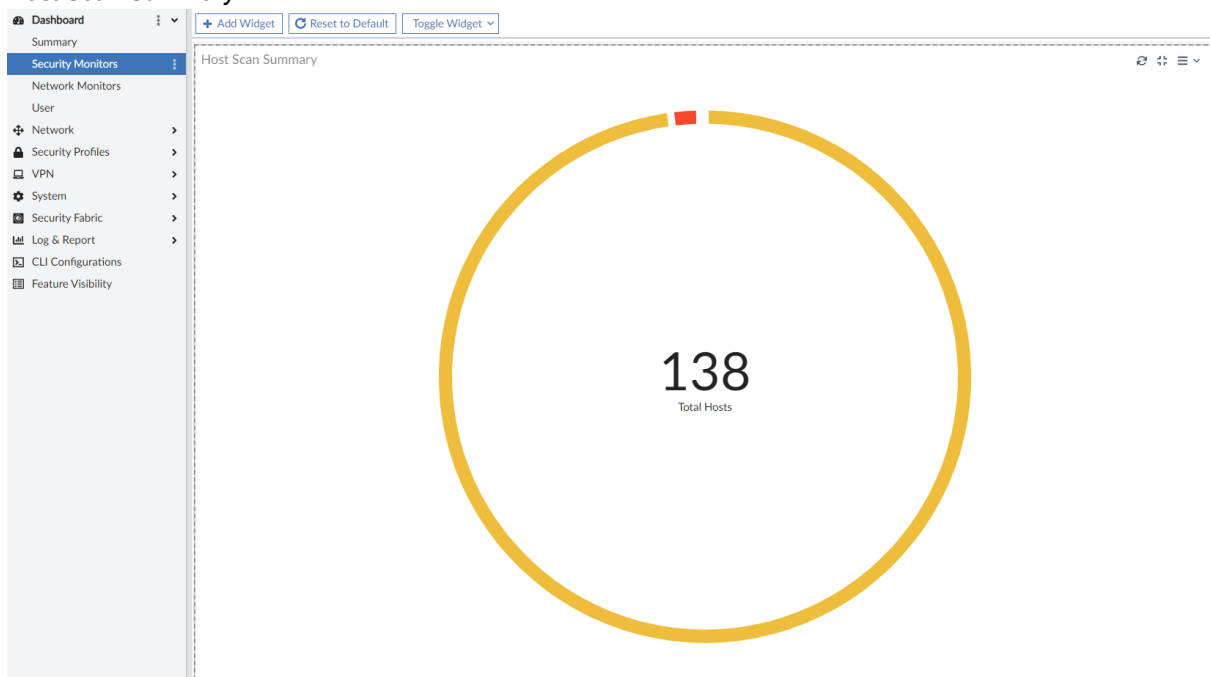


- **CPU and Memory Usage:**

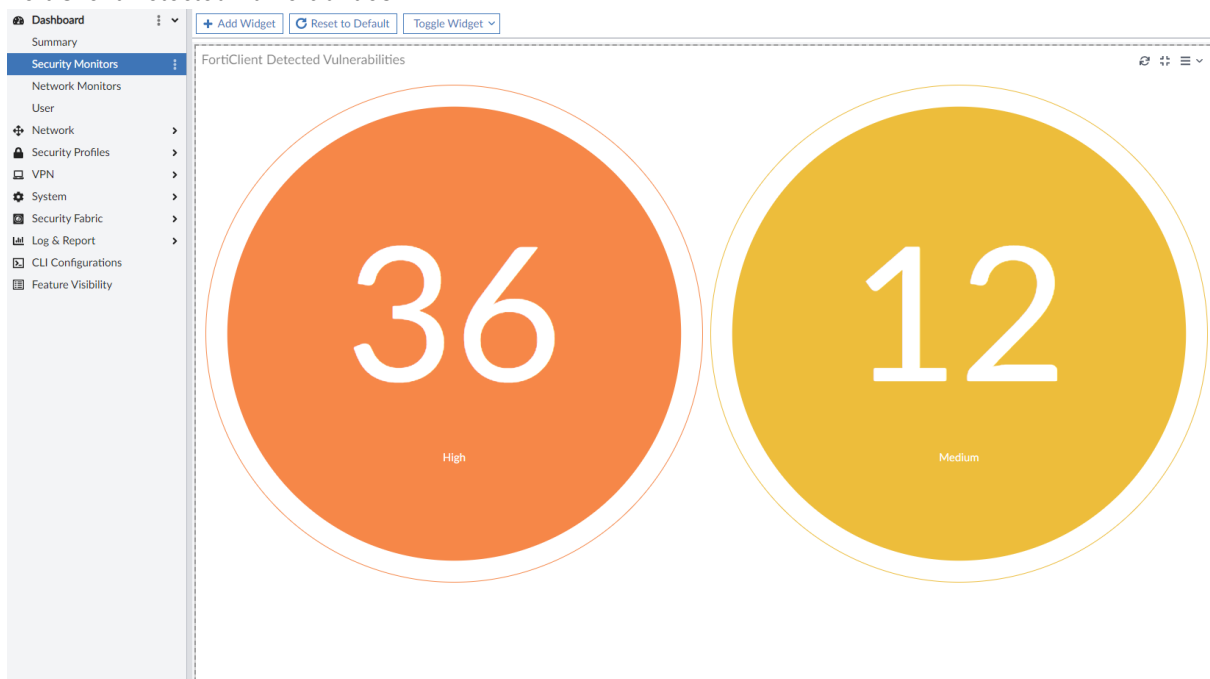
- The memory chart has been changed from a line chart to an area chart.
- The CPU chart shows the usage of each CPU for multi-CPU devices.



- **Host Scan Summary:**



- **FortiClient Detected Vulnerabilities:**



- **IPSEC VPN Widget:**

- The icon is red when the tunnel is down.
- The widget shows progress bars for incoming and outgoing traffic.

The IPsec VPN widget displays a table of VPN tunnels. The top screenshot shows two tunnels in a 'down' state, while the bottom screenshot shows them in an 'up' state with active traffic.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors	Created
20-21	10.2.170.21		0.0 KB	0.0 KB	20-21	20-21	Minute ago
20-27	10.2.170.27		0.0 KB	0.0 KB	20-27	20-27	Minute ago

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors	Created
20-21	10.2.170.21		840.0 B	840.0 B	20-21	20-21	Minute ago
20-27	10.2.170.27		420.0 B	420.0 B	20-27	20-27	Minute ago

Firewall Objects

- The create new/edit firewall address page uses tabs instead of a dropdown list for the address type *Category*.

Create New Address

Category: Address | IPv6 Address | Proxy Address

Name:

Color: Change

Type: Subnet

IP/Netmask:

Interface:

Static Route Configuration: ☐

Comments:

Add To Groups: Click to select

OK Cancel

- The create new/edit Virtual IP page uses tabs instead of a dropdown list for the *VIP Type*.

Create New Virtual IP

VIP Type: IPv4 | IPv6

Name:

Comments:

Color: Change

Status: ☒

Interface:

Configure Default Value: ☒

Network

Type: Static NAT | DNS Translation | FQDN | Load balance

External IP Address/Range:

Mapped IPv4 Address/Range:

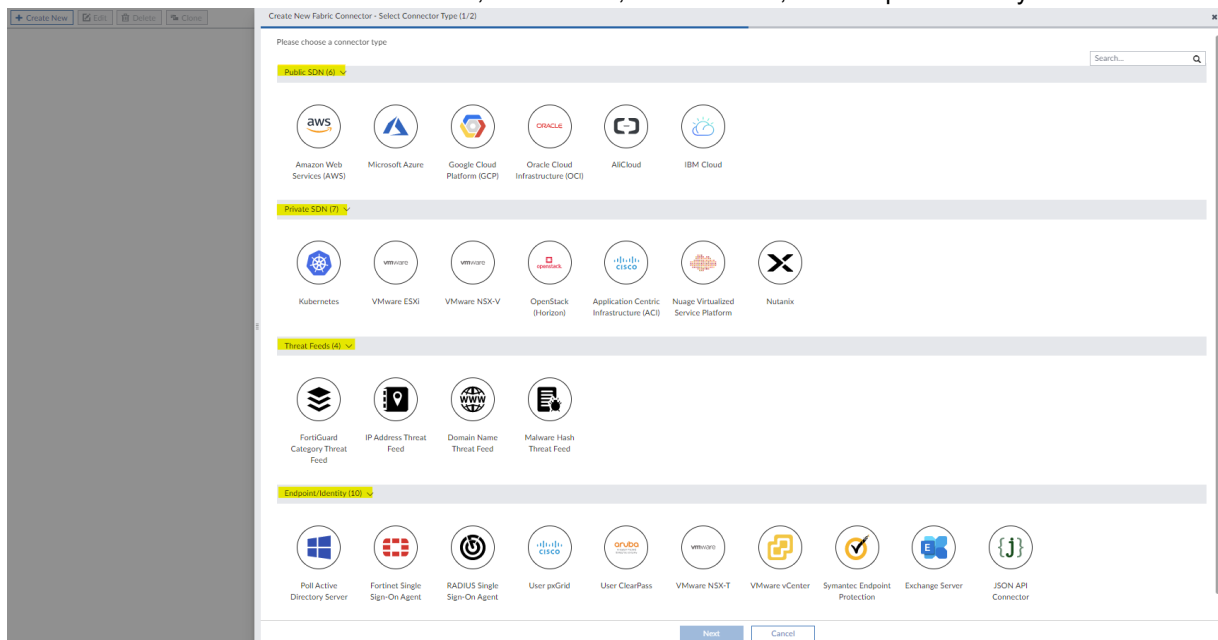
Mapped IPv6 Address/Range:

External IP Address/Range:

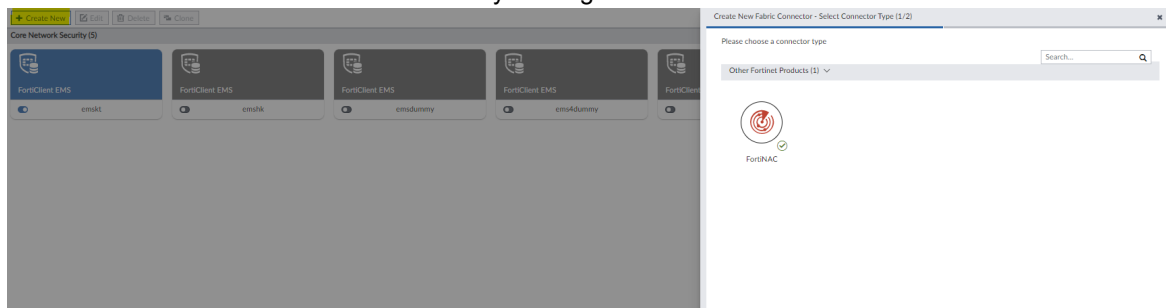
OK Cancel

Fabric Connector

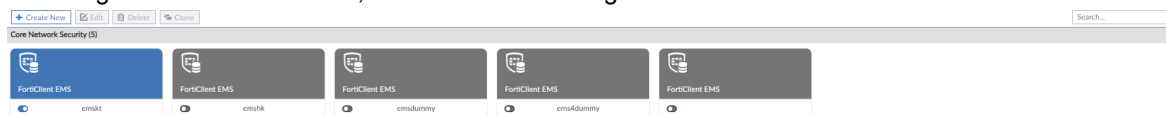
- Fabric connectors are reorganized by *Fabric Connectors* and *External Connectors*.
- External Connectors includes Private SDN, Public SDN, Threat Feeds, and Endpoint/Identity.



- Fabric Connectors include EMS and FortiNAC connectors.
- You can create a new FortiNAC connector by clicking *Create New*.



- To configure an EMS connector, edit one of the existing default EMS connectors.



- Users can also create fabric connectors from *Policy & Objects* by going to *Policy & Objects > Security Fabric* and selecting the *Fabric Connectors*, *SDN Connectors*, or *Endpoint/Identity* tabs.

Firewall Policies

- In firewall policies, the *Source* field groups *Address*, *User*, and *Internet Service* into one field with separate tabs.

The screenshot shows the 'Create New Firewall Policy' dialog box. The 'Source' field is selected, and the 'Address' tab is active in the 'Select Entries' panel. The 'Address' tab lists various entries, including 'all', 'gmail.com', 'login.microsoft.com', 'login.microsoftonline.com', 'login.windows.net', 'metadata-server', 'none', 'wildcard.dropbox.com', and 'wildcard.google.com'. The 'Destination' field is set to 'all', and the 'Service' field is set to 'ALL'.

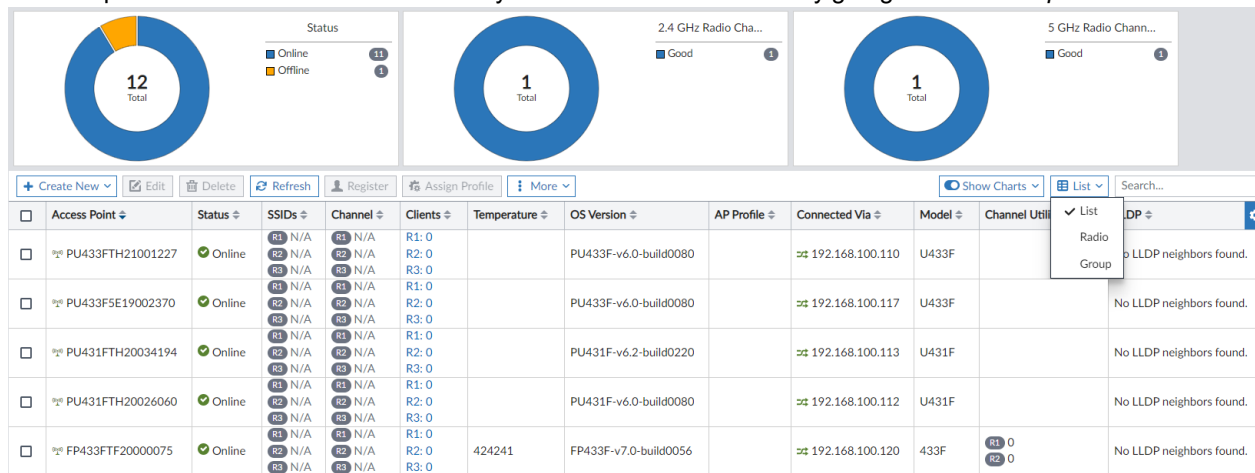
- Policy profiles have been made easier to find.

The screenshot shows the 'Create New Firewall Policy' dialog box. The 'Security Profiles' section is visible, showing a list of profile types: AntiVirus Profile, Web Filter Profile, DNS Filter, Application Control, IPS, File Filter, Email Filter, DLP Profile, VOIP, ICAP, SSH Filter, and SSL/SSH Inspection. The 'AntiVirus Profile' is selected, and the 'Profile Type' is set to 'Use Standard Security Profiles'.

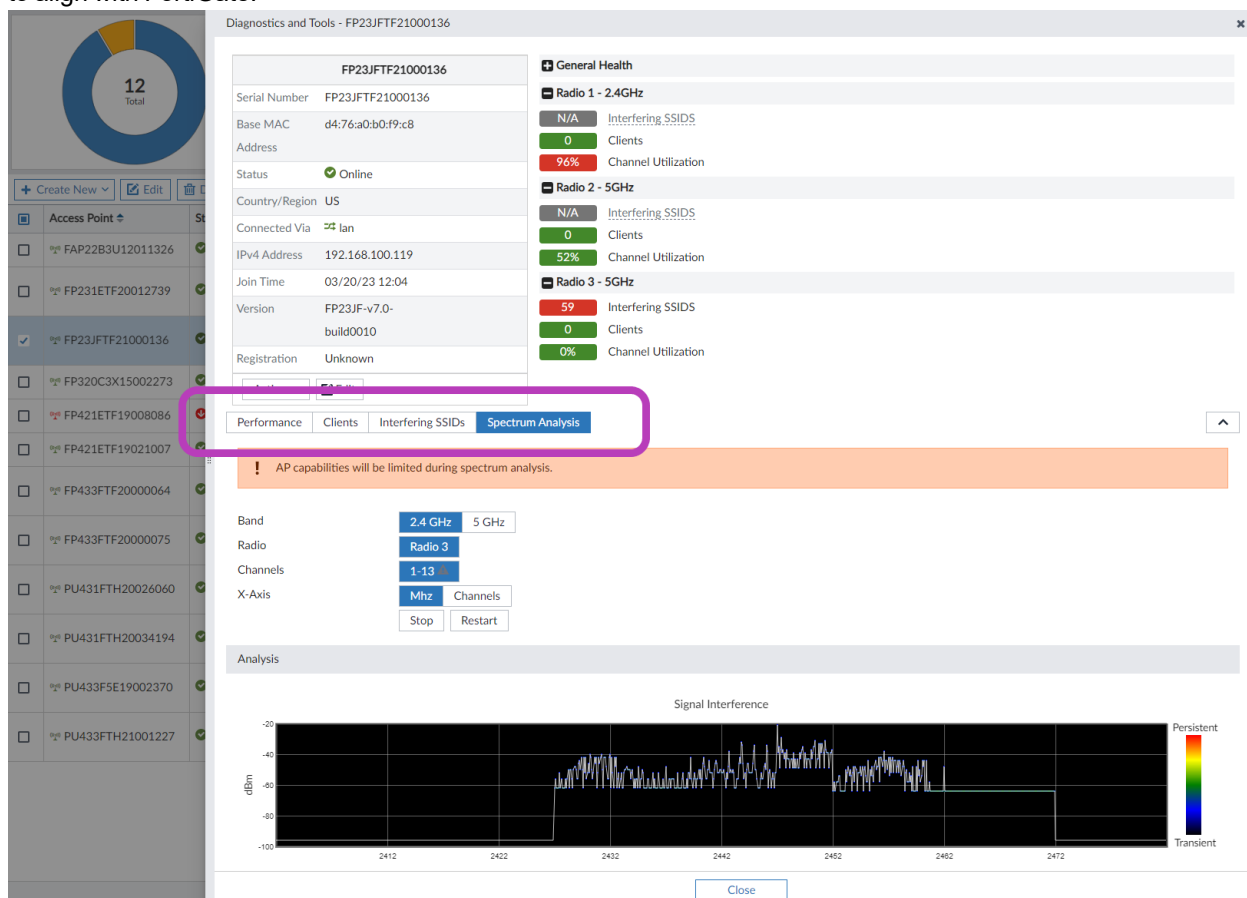
FortiAP Manager

- The different graphics, colors, and icons in FortiManager are aligned with the design of FortiGate. The changes include graphics, AP icon, channel utilization, diagnostics and tools, and AP groups.

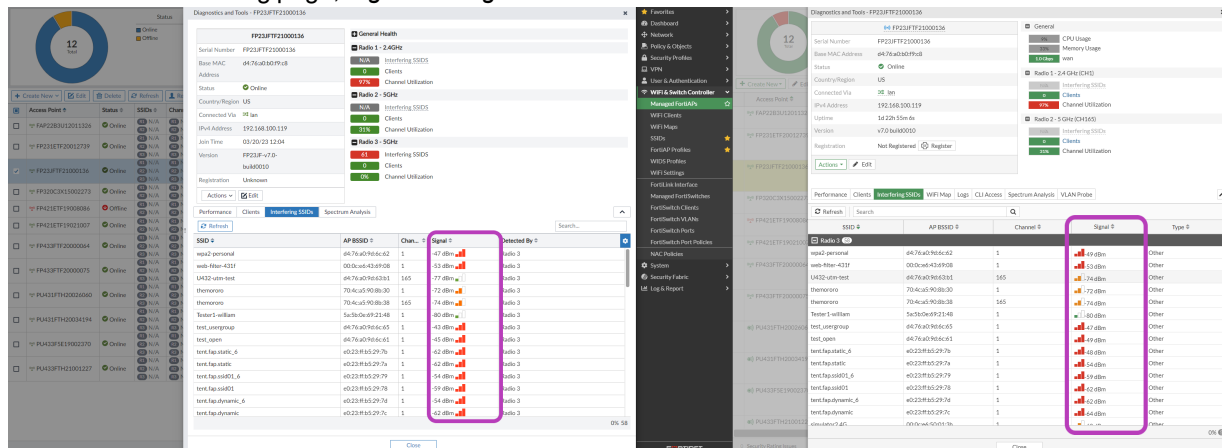
- AP Groups are not shown in the table view by default. You can enable it by going to *List > Group* in the toolbar.



- An empty space under the *Diagnostics and Tools* menu no longer exists, and the *Summary* tab has been removed to align with FortiGate.

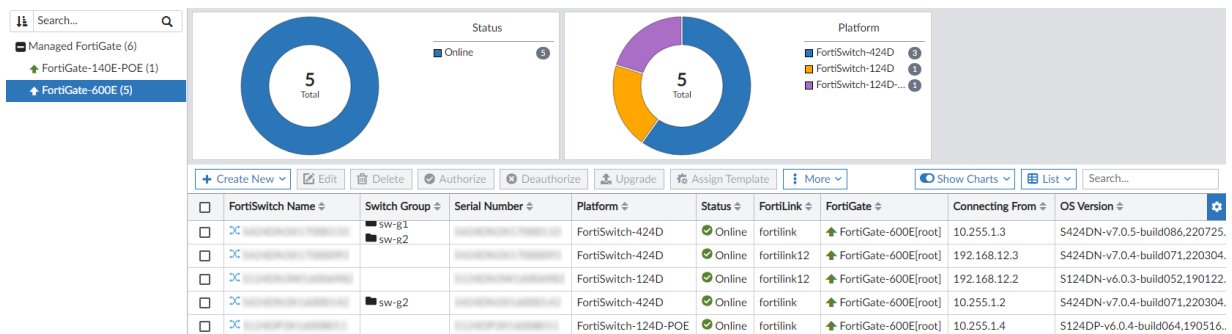


- On the client monitoring page, **Signal Strength** and **Rate Calculation** issues are resolved.

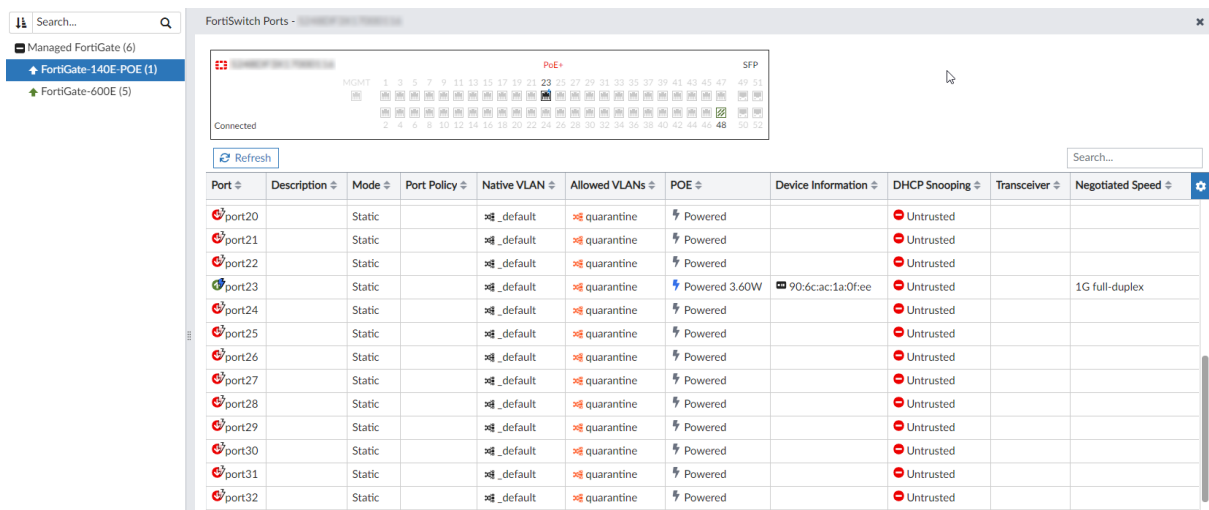


FortiSwitch Manager

- Enhancements have been made to the layout of the FortiSwitch Manager page.
- General.



- FortiSwitch Ports.



- Diagnostics & Tools.

The screenshot displays the FortiManager interface. On the left, a sidebar shows a search bar and a list of managed devices: Managed FortiGate (6), FortiGate-140E-POE (1), and FortiGate-600E (5). The main area is titled 'Diagnostics and Tools' and shows the status of a specific device, S424DN3X17000093. The status is 'Online' with a '5 Total' indicator. Below this, a table lists FortiSwitches with columns for FortiSwitch Name, Switch Group, and Serial Number. The right panel shows system health metrics: General (Good), CPU Usage (10%), Memory Usage (19%), Connection Uptime (103 day(s)), and Temperature (32°C). Below these, a 'Faceplate' section shows a network diagram. At the bottom, a 'Ports' section displays a table of port configurations.

Port	Description	Mode	Port Policy	Native VLAN	Allowed VLANs	POE	Device Information
port1		Static		default.33	quarantine.33		
port2		Static		default.33	quarantine.33		
port3		Static		default.33	quarantine.33		
port4		Static		default.33	quarantine.33		
port5		Static		default.33	quarantine.33		
port6		Static		default.33	quarantine.33		

FortiManager imports EPGs entries using the Cisco ACI connector as individual objects

FortiManager imports EPGs entries using the Cisco ACI connector as individual objects.

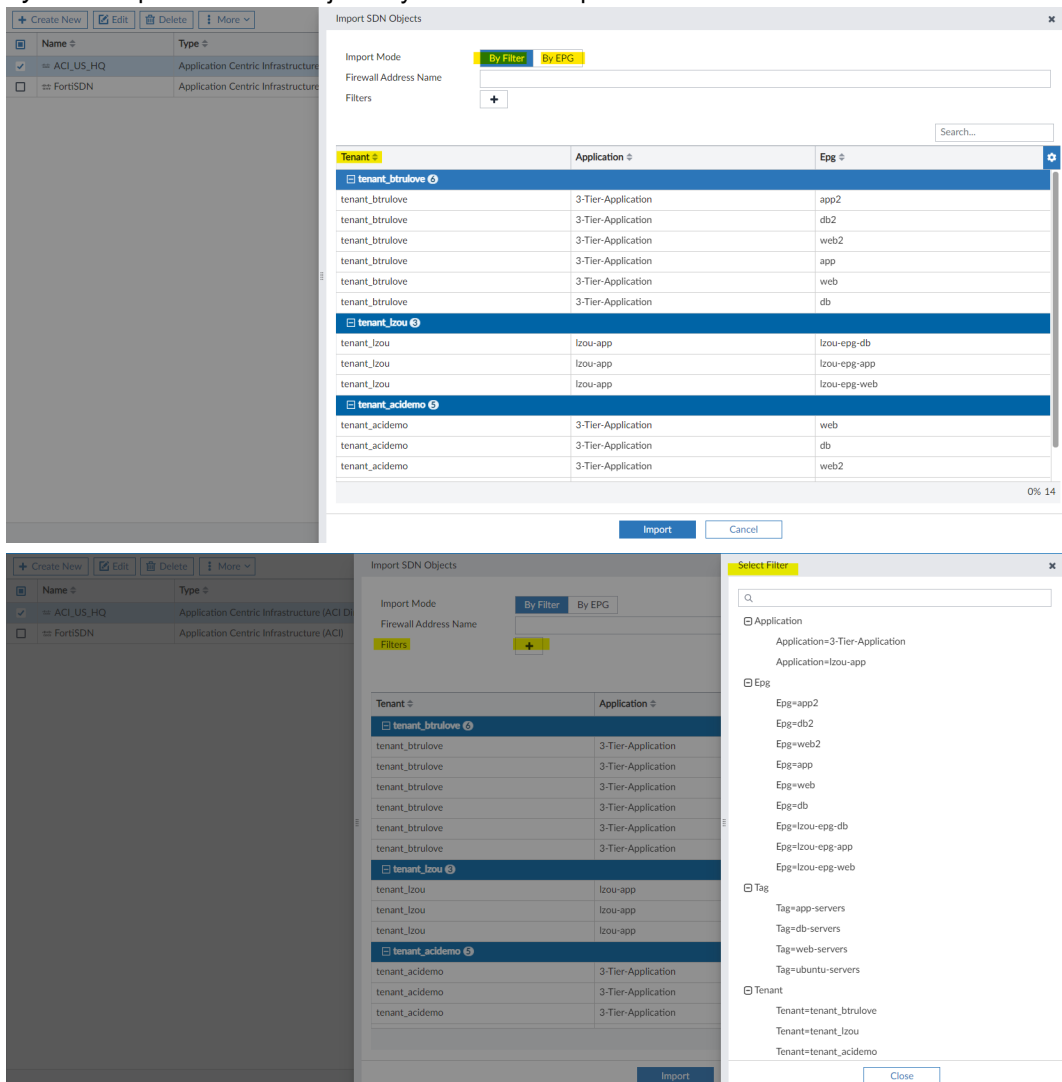
In order to import Endpoint Groups (EPGs) from ACI using the process described below, you must have already configured your Cisco APIC server.

To import EPGs as standalone objects from an ACI connector:

1. In FortiManager, configure the Application Centric Infrastructure (ACI) connector to use the *Direct Connection* ACI Type.
2. After configuring the remaining connector settings, you can import the SDN objects from *Policy & Objects > Object Configurations > External Connectors > Private SDN*, by right-clicking on the newly created Cisco ACI connector and choosing *Import*.

The import function loads all objects from the APIC server.

3. In the *Import SDN Objects* dialog, the *Import Mode* setting includes two modes: *By Filter* and *By EPG*.
- *By Filter*: Imports the SDN objects by filter. Click the plus icon to add filters.



- **By EPG:** This new setting allows you to import the SDN objects by Endpoint Group (EPG).

Import SDN Objects

Import Mode: By Filter **By EPG**

Firewall Address Name	Tenant	Application	Epg
tenant_btrulove			
ACItenant_btrulove3-Tier-Applicationapp2	tenant_btrulove	3-Tier-Application	app2
ACItenant_btrulove3-Tier-Applicationdb2	tenant_btrulove	3-Tier-Application	db2
ACItenant_btrulove3-Tier-Applicationweb2	tenant_btrulove	3-Tier-Application	web2
ACItenant_btrulove3-Tier-Applicationapp	tenant_btrulove	3-Tier-Application	app
ACItenant_btrulove3-Tier-Applicationweb	tenant_btrulove	3-Tier-Application	web
ACItenant_btrulove3-Tier-Applicationdb	tenant_btrulove	3-Tier-Application	db
tenant_lzou			
ACItenant_lzou3-Tier-Applicationlzhou-app-epg-db	tenant_lzou	lzhou-app	lzhou-epg-db
ACItenant_lzou3-Tier-Applicationlzhou-app-epg-app	tenant_lzou	lzhou-app	lzhou-epg-app
ACItenant_lzou3-Tier-Applicationlzhou-app-epg-web	tenant_lzou	lzhou-app	lzhou-epg-web
tenant_acidemio			
ACItenant_acidemio3-Tier-Applicationweb	tenant_acidemio	3-Tier-Application	web
ACItenant_acidemio3-Tier-Applicationdb	tenant_acidemio	3-Tier-Application	db
ACItenant_acidemio3-Tier-Applicationweb2	tenant_acidemio	3-Tier-Application	web2
ACItenant_acidemio3-Tier-Applicationdb2	tenant_acidemio	3-Tier-Application	db2
ACItenant_acidemio3-Tier-Applicationapp	tenant_acidemio	3-Tier-Application	app

Import Cancel

- You can create address objects from **Policy & Objects > Object Configurations > Firewall Objects** and use the address in a Policy Package, similar to other SDN connectors.

Edit Firewall Address

Name: aci-epg-db2

Color: [Color Picker]

Type: Dynamic

Sub Type: Fabric Connector Address

SDN Connector: ACI_US_HQ

SDN Address Type: Private

Filter: Epg=db2

Interface: any

Static Route Configuration: [Disabled]

Comments:

Add To Groups:

Advanced Options >

Per-Device Mapping >

Revision:

Change Note:

OK Cancel

The screenshot shows the FortiManager interface with the 'Edit Firewall Policy' window open. The left pane displays a list of policies, and the right pane shows the configuration for policy 1, 'DEMO'.

Policy List (Left Pane):

#	Name	From	To	Source
1	DEMO	any	any	aci-epg-db2 aci-test123 aci-test124 test-aci
Implicit (2/2 Total:1)				
2	Implicit Deny	any	any	all all

Policy Configuration (Right Pane):

ID: 1

Name: DEMO

Incoming Interface: any

Outgoing Interface: any

Source: aci-epg-db2, aci-test123, aci-test124, test-aci

Negate Source: Off

IP/MAC Based Access Control: Off

Destination: all

Negate Destination: Off

Service: ALL

Schedule: always

Action: Accept, Deny, IPSEC

Disclaimer Options: OK, Cancel

Index

The following index provides a list of all new features added to FortiManager 7.4. The index allows you to quickly identify the version where the feature first became available in FortiManager.

Select a version number to navigate in the index to the new features available for that release:

- [7.4.0 on page 144](#)
- [7.4.1 on page 145](#)

7.4.0

Device Manager

SD-WAN	<ul style="list-style-type: none">• Automated SD-WAN post overlay process creates policies to allow the health-checks traffic to flow between Branch and HUB on page 12• Automated SD-WAN overlay process adds "branch_id" meta variable auto assignment on page 15• SD-WAN monitoring map integrates with Cloud Assisted Monitoring Service to allow FortiGate interface speed tests from inside FortiManager on page 16• SDWAN monitoring map enhancements on page 19• SDWAN template for heterogeneous WAN link types on page 23
Templates	<ul style="list-style-type: none">• Preview CLI configuration for the device provisioning templates on page 25• Fortinet factory-default wireless and extender templates on page 28• Jinja Templates have direct access to the device DB to support generation of dynamic configuration on page 34

Central Management

FortiSwitch Manager	<ul style="list-style-type: none">• Per-device VRRP mapping can be used under FortiSwitch Profiles on page 50• FortiManager allows switchport export to another VDOM, and configuration of the exported port in the destination VDOM on page 51• FortiSwitch replacement procedure can be executed from FortiManager GUI on page 54
Other enhancements	<ul style="list-style-type: none">• FortiManager supports install preview for model devices on page 59• VPN Monitoring displays IPsec VPN tunnels created by IPsec templates and SD-WAN overlay wizard on page 64• FortiManager supports CLI diff in the workflow approval sessions on page 67

Policy and Objects

- | | |
|--------|---|
| Policy | <ul style="list-style-type: none">• Install preview support for partial install on page 71• Policy Package installation added link to the progress report page for installation errors on page 78• Support for IoT Virtual Patching in NAC policies using pre-built severity filters on page 82 |
|--------|---|

System

- | | |
|--------------------|---|
| High availability | <ul style="list-style-type: none">• FortiManager supports different VM type platforms to form the FortiManager cluster on page 92 |
| Other enhancements | <ul style="list-style-type: none">• Block out contract device from upgrading to next or major or minor release on page 100 |

Cloud Services

- | | |
|----------------|---|
| Cloud services | <ul style="list-style-type: none">• FortiManager used as single-pane management tool to orchestrate FortiGate deployment in AWS on page 105 |
|----------------|---|

Other

- | | |
|--------------------|---|
| Other enhancements | <ul style="list-style-type: none">• New FortiManager UX design on page 111• Fabric and External connector pages have been reorganized for an enhanced user experience on page 121• FortiManager connector relay to AWS will proxy all individual FortiGate requests on page 125• FortiManager key areas have been reorganized to enhance user experience on page 126• FortiManager imports EPGs entries using the Cisco ACI connector as individual objects on page 140 |
|--------------------|---|

7.4.1

Device Manager

- | | |
|-------------------|--|
| Device and groups | <ul style="list-style-type: none">• Auto-link setting is exposed to control configuration installation during ZTP 7.4.1 on page 8 |
| Templates | <ul style="list-style-type: none">• Fabric Authorization Template is integrated with Device Blueprint and supports meta variables 7.4.1 on page 41 |

Central Management

AP Manager	<ul style="list-style-type: none">• Multiple optimizations to the factory default SSID and AP-profiles 7.4.1 on page 46
FortiSwitch Manager	<ul style="list-style-type: none">• Custom commands can be assigned/unassigned at once to multiple managed FortiSwitches 7.4.1 on page 56
Other enhancements	<ul style="list-style-type: none">• Internet Service database update occurs only if specific policy objects require a FortiGuard update 7.4.1 on page 69

Policy and Objects

Policy	<ul style="list-style-type: none">• Policy deletion warning message improved with selected policy number and name reference 7.4.1 on page 83• Enable option for persistent policy hit-count on ADOM database 7.4.1 on page 84• Partial install pushes only the instructed configuration (JSON API) 7.4.1 on page 85• Policy partial install supports policy reorder/move operation (JSON API) 7.4.1 on page 87
--------	--

System

ADOM	<ul style="list-style-type: none">• ADOM 7.2 Policy Package supports installation on FortiGate 7.4 7.4.1 on page 93• 7.2 ADOM managing mixed FOS versions 7.4.1 on page 96• FortiManager can upgrade multiple ADOMs (same version) at the same time 7.4.1 on page 98
Other enhancements	<ul style="list-style-type: none">• Automatic system backup setup in GUI to configure a backup schedule and visualize backup history 7.4.1 on page 102



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.